Київський столичний університет імені Бориса Грінченка

Факультет журналістики

Кафедра міжнародної журналістики

«ЗАТВЕРДЖУЮ»
Проректор з науково-педагогічної
та навчальної роботи
_____ О.Б. Жильцов
«__ * __» _____ 2026 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інформаційні війни у світових медіа

для студентів

рівня вищої освіти першого (бакалаврського)

вибіркова навчальна дисципліна

КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Код ЄДРПОУ 45307966
Програма № 3108/26
Начальник відділу моніторингу якості освіти
(підпис) (прізвище, ініціали)
«__» 20 26 р.

Київ – 2026

Розробник:
Мураховський Денис Анатолійович, викладач кафедри міжнародної журналістики

Викладач:
Мураховський Денис Анатолійович, викладач кафедри міжнародної журналістики

Робочу програму розглянуто і затверджено на засіданні кафедри міжнародної журналістики Факультету журналістики

Протокол від «30» січня 2026 року № 6

Завідувач кафедри _____ Віталій ТЕРЕЩУК

Робочу програму перевірено
_____ . _____ . 2026 р.
Заступник декана _____ Роксолана ДЬЯЧЕНКО

Пролонговано:

на 20__/20__ н.р. _____(_____). «___»_____20__р., протокол №___

на 20__/20__ н.р. _____(_____). «___»_____20__р., протокол №___

на 20__/20__ н.р. _____(_____). «___»_____20__р., протокол №___

на 20__/20__ н.р. _____(_____). «___»_____20__р., протокол №___

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Найменування показників	**Характеристика дисципліни за формами навчання**
	денна
Вид дисципліни	вибіркова
Мова викладання, навчання та оцінювання	українська
Загальний обсяг кредитів/годин	4 / 120
Курс	3
Семестр	6
Кількість змістових модулів за розподілом	4
Обсяг кредитів	4
Обсяг годин, в тому числі:	120
аудиторні	56
модульний контроль	8
семестровий контроль	–
самостійна робота	56
Форма семестрового контролю	залік

2. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Мета дисципліни — сформувати у студентів системне розуміння природи інформаційних війн, механізмів пропаганди, дезінформації, психологічних операцій, інструментів впливу у глобальному медіапросторі, а також здатність аналізувати інформаційні атаки на держави, інституції та суспільства.

Предмет вивчення — форми, стратегії та технології ведення інформаційних війн у світі, їхня роль у міжнародних комунікаціях, політиці, безпеці та медіа.

Основні **завдання** дисципліни:

- дослідити теоретичні засади інформаційних війн;
- навчити розпізнавати моделі пропаганди та маніпуляцій;
- вивчити інструменти та технології дезінформації;
- дослідити історичні та сучасні кейси інформаційних операцій;
- сформувати навички аналізу інформаційних кампаній різних держав;
- оцінювати інформаційні загрози національній та глобальній безпеці;
- зрозуміти роль медіа у формуванні когнітивного та стратегічного впливу.

Впродовж вивчення дисципліни, студенти отримують такі **компетентності** відповідно до освітньої програми «Міжнародна журналістика»:

загальні:

- **ЗК02** Знання та розуміння предметної області та розуміння професійної діяльності;
- **ЗК04** Здатність до пошуку, оброблення та аналізу інформації з різних джерел;
- **ЗК05** Навички використання інформаційних та комунікаційних технологій;
- **ЗК07** Здатність працювати в команді;
- **ЗК10** Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

фахові:

- **СК01**. Здатність застосовувати знання зі сфери соціальних комунікацій у своїй професійній діяльності;
- **СК02**. Здатність формувати інформаційний контент.

3. РЕЗУЛЬТАТИ НАВЧАННЯ ЗА ДИСЦИПЛІНОЮ

У результаті вивчення навчальної дисципліни **здобувач повинен**

знати:

– історію становлення інформаційних війн;
– моделі пропаганди (Герман–Хомскі, Лассвелл, Бернейс тощо);
– типи дезінформаційних кампаній та фейків;
– роль медіа в інформаційних конфліктах;
– інформаційні стратегії держав світу;
– вплив технологій (AI, deepfake, соцмережі, боти, тролі) на інформаційні війни;
– механізми гібридних операцій РФ, Китаю, Ірану, США тощо.

уміти:

– розпізнавати інформаційні атаки та медіаманіпуляції;
– аналізувати структуру та воронку інформаційних впливів;
– працювати з OSINT-інструментами;
– ідентифікувати інформаційні наративи та пропагандистські техніки;
– відрізняти факти від інформаційних конструктів;
– створювати аналітичні огляди інформаційних кампаній;
– оцінювати рівень інформаційної загрози.

Впродовж вивчення дисципліни мають бути досягнуті такі **програмні результати навчання**:

– **ПР02**. Застосовувати знання зі сфери предметної спеціалізації для створення інформаційного продукту чи для проведення інформаційної кампанії;
– **ПР04**. Виконувати пошук, оброблення та аналіз інформації з різних джерел;
– **ПР08**. Виокремлювати у виробничих ситуаціях факти, події, відомості, процеси, про які бракує знань, і розкривати способи та джерела здобування тих знань;
– **ПР13**. Передбачати реакцію аудиторії на інформаційний продукт чи на інформаційні акції, зважаючи на положення й методи соціальнокомунікаційних наук;
– **ПР18**. Використовувати необхідні знання й технології для виходу з кризових комунікаційний ситуацій на засадах толерантності, діалогу й співробітництва.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторні					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Теоретичні засади інформаційних війн							
Тема 1. Термінологія та концепції інформаційних війн	4	2		2			
Тема 2. Моделі та стратегії впливу: від Бернейса до цифрових війн XXI століття	22	2		2	2		16
Тема 3. Інформаційні екосистеми та глобальні медіаплатформи як простір для ІПСО	6	2		2	2		
Модульний контроль	2						
Разом	34	6		6	4		16
Змістовий модуль 2. Інформаційні війни у світі: історичні та сучасні кейси							
Тема 4. Історичний контекст інформаційних війн	12	2		2			8
Тема 5. Інформаційні війни: глобальні кейси XXI століття	4	2		2			
Тема 6. Гібридні інформаційні операції та державні стратегії впливу у XXI столітті	4	2		2			
Модульний контроль	2						
Разом	22	6		6			8
Змістовий модуль 3. Технології інформаційних війн у цифрову епоху							
Тема 7. Цифрові інструменти інформаційних атак	22	2		2	2		16
Тема 8. Масштабні дезінформаційні кампанії у світі: методи, інструменти, платформи	4	2		2			
Тема 9. Кіберпростір і інформаційні кібероперації як складова сучасних війн	6	2		2	2		
Модульний контроль	2						
Разом	34	6		6	4		16
Змістовий модуль 4. Україна в умовах інформаційної війни							
Тема 10. Інформаційні операції проти України	20	2		2			16
Тема 11. Українські стратегії протидії дезінформації та інформаційним атакам	4	2			2		
Тема 12. Міжнародний вимір інформаційної війни проти України	4	2			2		
Модульний контроль	2						
Разом	30	6		2	4		16
РАЗОМ	120	24		20	12		56

5. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Змістовий модуль 1.
Теоретичні засади інформаційних війн

Тема 1. Термінологія та концепції інформаційних війн

Пропаганда, дезінформація, інформаційна операція, ІПСО; історичні моделі маніпуляцій; інформаційна війна як інструмент державної політики.

Рекомендовані джерела: основні – 1 ,2, 3, 4; додаткові – 2, 4, 6, 10.

Тема 2. Моделі та стратегії впливу: від Бернейса до цифрових війн XXI ст.

PR як маніпулятивний інструмент, психологічні операції: структура, етапи, когнітивний вплив, нейропсихологія пропаганди.

Рекомендовані джерела: основні – 1 ,2, 3, 4; додаткові – 2, 4, 6, 10.

Тема 3. Інформаційні екосистеми та глобальні медіаплатформи як простір для ІПСО

Роль соціальних мереж у формуванні інформаційних потоків, алгоритмічні «воронки впливу» та фільтр-бульбашки, ботмережі, тролеферми, фабрики контенту; механізми поширення фейків і вірусних наративів; інформаційна зброя в екосистемах TikTok, X, Telegram, YouTube.

Рекомендовані джерела: основні – 1 ,2, 3, 4; додаткові – 2, 4, 6, 10.

Змістовий модуль 2.
Інформаційні війни у світі: історичні та сучасні кейси

Тема 4. Історичний контекст інформаційних війн

Поняття «інформаційна війна» в історичній перспективі. Еволюція інструментів інформаційного впливу від античності до XX століття. Нацистська пропаганда та її моделі. Радянська школа дезінформації та «активні заходи» КДБ. Інформаційні операції під час холодної війни. Аналіз застосування інформаційних технологій у війнах у Югославії, Іраку та Афганістані. Історичні закономірності, що визначили сучасну конфігурацію інформаційних війн.

Тема 5. Інформаційні війни: глобальні кейси XXI століття

Масштабні інформаційні операції у світі після 2000 року. Вплив соціальних мереж на протестні рухи та революційні процеси (Арабська весна). Інформаційні атаки та спроби зовнішнього втручання у виборчі процеси (вибори США 2016 року). Інформаційні кампанії під час Brexit. Особливості застосування інформаційного впливу Китаєм у країнах Азії та Африки. Порівняльний аналіз підходів різних держав до інформаційних стратегій у глобальному середовищі.

Рекомендовані джерела: основні – 4, 6, 7; додаткові – 6, 10, 11, 12.

Тема 6. Гібридні інформаційні операції та державні стратегії впливу у XXI столітті

Поняття гібридної війни та її інформаційно-психологічна складова. Доктрина Ґерасимова та російська модель поєднання військових, політичних та інформаційних інструментів. Інформаційні операції Ірану: релігійні наративи, мережеві впливи, кіберкомпонента. Інформаційні стратегії Туреччини та моделі контролю медіапростору. Механізми інформаційного суверенітету Китаю: цензура, контроль потоків інформації, формування керованих наративів. Аналіз сучасних конфліктів (Сирія, Нагірний Карабах, Сахель) як прикладів гібридного поєднання інформаційних та військових інструментів.

Рекомендовані джерела: основні – 4, 6, 7; додаткові – 6, 10, 11, 12.

Змістовий модуль 3.
Технології інформаційних війн у цифрову епоху

Тема 7. Цифрові інструменти інформаційних атак

Соціальні мережі як середовище поширення інформаційних впливів. Алгоритми платформ та їх роль у формуванні інформаційних потоків. Ботмережі, тролеферми та координована неавтентична поведінка. Синтетичні медіа та deepfake як інструменти дестабілізації. Використання штучного інтелекту у виробництві та масштабуванні маніпулятивного контенту. Особливості цифрових кампаній у TikTok, X, Telegram та YouTube.

Рекомендовані джерела: основні – 1, 3, 5, 6; додаткові – 4, 5, 9, 11, 13.

Тема 8. Масштабні дезінформаційні кампанії у світі: методи, інструменти, платформи

Глобальні приклади дезінформаційних операцій, реалізованих різними державами та недержавними акторами. Канали та механізми поширення наративів у міжнародному медіапросторі. Платформи, що найчастіше використовуються для інформаційних кампаній, та їх уразливості. Техніки маніпуляції, що застосовуються у великих інформаційних операціях. Аналіз відомих кейсів та їхніх методологічних особливостей.

Рекомендовані джерела: основні – 1, 3, 5, 6; додаткові – 4, 5, 9, 11, 13.

Тема 9. Кіберпростір і інформаційні кібероперації як складова сучасних війн

Взаємодія кібероперацій та інформаційних операцій у сучасних конфліктах. Основні типи кіберзагроз: APT-групи, хактивізм, атаки на критичну інфраструктуру. Операції типу hack-and-leak як інструмент політичного та інформаційного тиску. Роль кіберрозвідки та OSINT у виявленні та документуванні інформаційно-кіберних атак. Приклади комплексних операцій: Sony Hack, NotPetya, атаки на енергомережі різних країн. Формування кіберстійкості держав та суспільств.

Рекомендовані джерела: основні – 1, 3, 5, 6; додаткові – 4, 5, 9, 11, 13.

Змістовий модуль 4
Україна в умовах інформаційної війни

Тема 10. Інформаційні операції проти України

Наративи РФ, спрямовані на деморалізацію, паніку та розкол суспільства. Основні інформаційні атаки на міжнародну репутацію України з 2014 року та під час повномасштабного вторгнення. Кампанії дискредитації Збройних сил України, державних інституцій, гуманітарних ініціатив і волонтерського руху. Методи поширення ворожих наративів у соціальних мережах, на міжнародних платформах та через агентів впливу.

Рекомендовані джерела: основні – 4, 5, 7; додаткові – 1, 3, 7, 8, 13.

Тема 11. Українські стратегії протидії дезінформації та інформаційним атакам

Система державної та недержавної протидії дезінформації в Україні: Центр протидії дезінформації, StratCom, медійні ініціативи громадянського суспільства. Інституційні та комунікаційні механізми стримування інформаційних загроз. Роль українських медіа, фактчек-проєктів і волонтерських груп. Побудова суспільної стійкості (resilience) через медіаграмотність, критичне мислення та стратегічні комунікації.

Рекомендовані джерела: основні – 4, 5, 7; додаткові – 1, 3, 7, 8, 13.

Тема 12. Міжнародний вимір інформаційної війни проти України

Глобальні інформаційні наративи про Україну та їх трансформація після 2014 і 2022 років. Протидія російському впливу в міжнародних медіа, аналітичних центрах, дипломатії та соцмережах. Роль ЄС, США, НАТО й міжнародних організацій у захисті інформаційного простору України. Санкції проти російських медіаструктур, обмеження діяльності RT і Sputnik. Стратегії інформаційної підтримки України на глобальному рівні та приклади ефективних міжнародних комунікаційних кампаній.

Рекомендовані джерела: основні – 4, 5, 7; додаткові – 1, 3, 7, 8, 13.

6. КОНТРОЛЬ НАВЧАЛЬНИХ ДОСЯГНЕНЬ

6.1. Система оцінювання навчальних досягнень студента

№	Вид діяльності	**Максимальна кількість балів за одиницю**	Модуль 1		Модуль 2		Модуль 3		Модуль 4	
			Кількість одиниць	**Максимальна кількість балів**	**Кількість одиниць**	**Максимальна кількість балів**	**Кількість одиниць**	**Максимальна кількість балів**	**Кількість одиниць**	**Максимальна кількість балів**
1.	Відвідування лекцій	1	3	3	3	3	3	3	3	3
2.	Відвідування практичних занять	1	3	3	3	3	3	3	1	1
3.	Робота на практичному занятті	10	3	30	3	30	3	30	1	10
4.	Відвідування лабораторних занять	1	2	2	0	0	2	2	2	2
5.	Робота на лабораторному занятті	10	2	20	0	0	2	20	2	20
6.	Виконання завдань самостійної роботи	5	1	5	1	5	1	5	1	5
7.	Виконання модульної контрольної роботи	25	1	25	1	25	1	25	1	25
Разом				88		66		88		66
Максимальна кількість балів: 308										
Розрахунок коефіцієнта: 308 / 100 = 3,08										

6.2. Завдання для самостійної роботи та критерії оцінювання

№ теми	**Завдання для самостійної роботи**	**К-ть годин**	**Бали**
Змістовий модуль 1			
2.	Пройти безкоштовний курс на платформі Prometheus «Інформаційні війни». URL: https://prometheus.org.ua/prometheus-free/information-wars/	16	5
Змістовий модуль 2			
4.	Підготувати доповідь на тему, присвячений окремому кейсу застосування технологій інформаційних війн у міжнародних відносинах. Приклади тем: – Інформаційні війни Античного періоду – Інформаційні війни часів Середньовіччя – Інформаційні війни під час боротьби США за незалежність – Інформаційні війни періоду Першої світової війни – Інформаційні війни на теренах Європи у міжвоєнний період (1920–1930-ті роки) – Інформаційні війни періоду Другої світової війни – Інформаційні війни періоду Холодної війни – Інформаційні війни у відносинах *Держава1* та *Держава2*	8	5

Змістовий модуль 3			
7.	Пройти безкоштовний курс на платформі Prometheus «Інформаційна безпека». URL: https://prometheus.org.ua/prometheus-free/інформаційна-безпека/	16	5
Змістовий модуль 4			
10.	Пройти безкоштовний курс на платформі Prometheus «Інформаційна гігієна під час війни». URL: https://prometheus.org.ua/prometheus-free/information-hygiene-during-war	16	5

Критерії оцінювання

Бал	Критерій
5	здобувач засвоїв теоретичний матеріал, який винесений на самостійну роботу, застосування для оформлення результатів самостійної роботи не тільки рекомендованої, а й додаткової літератури та творчого підходу; чітке володіння понятійним апаратом, теорією; вміння використовувати їх для виконання конкретних практичних завдань, розв'язання ситуацій. Оформлення результатів самостійної роботи повинно бути логічним та послідовним.
4	здобувач засвоїв теоретичний матеріал з відповідної теми який винесений на самостійну роботу, та наявне вміння орієнтуватися в ньому, усвідомлене застосування знань для розв'язання практичних задач; за умови виконання всіх вимог, які передбачено для оцінки «5 балів», при наявності незначних помилок або не зовсім повних висновків за одержаними результатами. Оформлення виконаного завдання з самостійної роботи має бути послідовним.
2–3	здобувач не повністю засвоїв тему для самостійного опрацювання не досконало володіє основними поняттями та положеннями навчальної дисципліни, невпевнено орієнтується в першоджерелах та рекомендованій літературі, непереконливо відповідає, додаткові питання викликають невпевненість або відсутність знань.
1	здобувач не опанував навчальний матеріал з відповідної теми для самостійного опрацювання, не знає основних понять і термінів наукової дисципліни, не орієнтується в першоджерелах та рекомендованій літературі, відсутнє наукове або логічне мислення.

6.3. Форма проведення модульного контролю та критерії оцінювання

Виконання модульних контрольних робіт здійснюється за допомогою засобів комп'ютерного тестування. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

Критерії оцінювання модульної контрольної роботи — максимум 25 балів за кожну модульну роботу.

6.4. Форми проведення семестрового контролю та критерії оцінювання

Підсумкове оцінювання знань здобувачів з дисципліни відбувається у формі заліку за підсумковою оцінкою з курсу.

6.5. Шкала відповідності оцінок

Оцінка	**Кількість балів**
відмінно	90–100
дуже добре	82–89
добре	75–81
задовільно	69–74
достатньо	60–68
незадовільно	0–59

7. НАВЧАЛЬНО-МЕТОДИЧНА КАРТКА ДИСЦИПЛІНИ

Разом 120 годин, у т.ч.: лекції — 24 год., лабораторні — 12 год., практичні заняття — 20 год., модульний контроль — 8 год., самостійна робота — 56 год.

Модулі (назви, бали)	Змістовий модуль 1 **Теоретичні засади інформаційних війн** (88 балів)			Змістовий модуль 2 **Історичний розвиток та глобальні кейси інформаційних воєн** (66 балів)		
Теми	1	2	3	4	5	6
Теми лекцій	Лекція 1. Термінологія та концепції інформаційних війн (1 бал)	Лекція 2. Моделі та стратегії впливу: від Бернейса до цифрових війн XXI століття (1 бал)	Лекція 3. Інформаційні екосистеми та глобальні медіаплатформи як простір для ІПСО (1 бал)	Лекція 4. Історичний контекст інформаційних війн (1 бал)	Лекція 5. Інформаційні війни: глобальні кейси XXI століття (1 бал)	Лекція 6. Гібридні інформаційні операції та державні стратегії впливу у XXI столітті (1 бал)
Теми лабораторних занять		Лабораторне заняття 1. Ідентифікація маніпулятивних технік у медіаконтенті (11 балів)	Лабораторне заняття 2. Аналіз інформаційних потоків та виявлення координації ботмереж у соцмережах (11 балів)			
Теми практичних занять	Практичне заняття 1. Аналіз пропаганди та дезінформації в медіа (11 балів)	Практичне заняття 2. Виявлення психологічних технік маніпуляції (11 балів)	Практичне заняття 3. Аналіз інформаційних екосистем та механізмів поширення фейків (11 балів)	Практичне заняття 4. Аналіз історичних інформаційних операцій (11 балів)	Практичне заняття 5. Дослідження глобальних інформаційних кейсів XXI століття (11 балів)	Практичне заняття 6. Моделювання гібридних інформаційних операцій сучасних держав (11 балів)
Самостійна робота		(5 балів)		(5 балів)		
Види поточного контролю	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)		

Модулі (назви, бали)	Змістовий модуль 3. **Цифрові інструменти та сучасні технології інформаційної боротьби** (88 балів)			Змістовий модуль 4 **Україна в умовах інформаційної війни** (66 балів)		
Теми	7	8	9	10	11	12
Теми лекцій	Лекція 7. Цифрові інструменти інформаційних атак (1 бал)	Лекція 8. Масштабні дезінформаційні кампанії у світі: методи, інструменти, платформи (1 бал)	Лекція 9. Кіберпростір і інформаційні кібероперації як складова сучасних війн (1 бал)	Лекція 10. Інформаційні операції проти України (1 бал)	Лекція 11. Українські стратегії протидії дезінформації та інформаційним загрозам (1 бал)	Лекція 12. Міжнародний вимір інформаційної війни проти України
Теми лабораторних занять	Лабораторне заняття 3. Виявлення ознак синтетичного контенту та deepfake у медіа (11 балів)		Лабораторне заняття 4. Аналіз структури та тактики APT-груп у контексті інформаційних війн (11 балів)		Лабораторне заняття 5. Ідентифікація та класифікація механізмів дезінформації, які використовуються проти України (11 балів)	Лабораторне заняття 6. Аналіз міжнародних медіаплатформ щодо формування глобальних наративів про Україну (11 балів)
Теми практичних занять	Практичне заняття 7. Аналіз інструментів цифрових інформаційних атак (11 балів)	Практичне заняття 8. Дослідження кіберінцидентів як елементів інформаційних операцій (11 балів)	Практичне заняття 9. Моделювання комплексної цифрової інформаційної атаки та сценаріїв її нейтралізації (11 балів)	Практичне заняття 10. Аналіз ворожих наративів, спрямованих проти України та оцінка ефективності стратегій протидії (11 балів)		
Самостійна робота	(5 балів)			(5 балів)		
Види поточного контролю	Модульна контрольна робота 3 (25 балів)			Модульна контрольна робота 4 (25 балів)		
Підсумковий контроль	ЗАЛІК					

8. РЕКОМЕНДОВАНІ ДЖЕРЕЛА

Основні (базові):

1. Почепцов Г. Сучасні інформаційні війни. 3-тє вид. Київ: Видавничий дім «Києво-Могилянська академія», 2016. 504 с.
2. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі: навчальний посібник. Київ: ВІКНУ, 2016. 286 с.
3. Гамова І. В. Інформаційні війни: підручник. Київ: Державний торговельно-економічний університет, 2022. 184 с.
4. Світова гібридна війна: український фронт: монографія / За заг. ред. В. П. Горбуліна. Київ: Національний інститут стратегічних досліджень, 2017. 494 с.
5. Сенченко М. І. Латентна світова інформаційна війна. Київ: ФОП Стебеляк, 2014. 384 с.
6. Магда Є. Гібридна агресія Росії: уроки для Європи. Київ: Каламар, 2017. 268 с.
7. Гула Р. В., Дзьобань О. П., Передерій І. Г., Павліченко О. О., Філь Г. О. Інформаційна війна: соціально-онтологічний та мілітарний аспекти: монографія. Київ: Каравела, 2020. 288 с.
8. Худолій А. О. Інформаційна війна 2014–2022 рр.: монографія. Острог: Вид-во Національного університету «Острозька академія», 2022. 208 с.
9. Pomerantsev, P. This Is Not Propaganda: Adventures in the War Against Reality. London: Faber & Faber, 2019.
10. Rid, T. Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux, 2020.
11. Benkler, Y., Faris, R., Roberts, H. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. Oxford: Oxford University Press, 2018.
12. Nye, J. S. Jr. Soft Power: The Means to Success in World Politics. New York: PublicAffairs, 2004.
13. Paul, C. Information Operations: Doctrine and Practice. A Reference Handbook. Westport, CT: Praeger Security International, 2008.

Додаткові:

1. Федотенко К. А. «Інформаційна війна» й «інформаційний фронт»: наукове осмислення понять // Вісник Національного юридичного університету імені Ярослава Мудрого. 2023. № 3 (58). С. 157–164.
2. Бучин М., Курус Ю. Інформаційна війна Росії проти України: особливості та механізми протидії // Гуманітарні візії. 2018. Т. 4, № 1. С. 55–62.
3. Шемчук В. В. Інформаційна безпека держави та інформаційна війна // Україна під час російсько-української війни 2014–2023 рр.: ґенеза національної

стійкості крізь призму наукових досліджень: монографія / за заг. ред. Б. Попкова, С. Пєткова. Київ: Ліра-К, 2023. С. 140–161.

4. Уздєнова Ю. М. Гібридна війна: сутність, складові та ключові поняття // Вчені записки ТНУ ім. В. І. Вернадського. Серія: Публічне управління та адміністрування. 2024. Т. 35 (74), № 4. С. 172–180.
5. Стратегічні комунікації в умовах гібридної війни: погляд від волонтера до науковця: монографія / [В. А. Азарова та ін. ; за заг. ред. Л. Ф. Компанцевої]. Київ: Національна академія Служби безпеки України, 2021. 499 с.
6. Баглікова М. Інформаційні війни і Україна // Науковий вісник Ужгородського університету : Серія: Політологія. Соціологія. Філософія. Ужгород: Видавництво УжНУ «Говерла», 2010. Вип. 14. С. 158–161.
7. EUvsDisinfo. Detecting, analysing, and raising awareness of pro-Kremlin disinformation. East Stratcom Task Force, European External Action Service. URL:https://euvsdisinfo.eu/
8. StopFake.org. Український фактчекінговий проєкт протидії дезінформації про події в Україні. URL: https://www.stopfake.org .
9. The Bellingcat. Bellingcat Online Open Source Investigation Toolkit та інші OSINT-ресурси. URL: https://www.bellingcat.com; https://bellingcat.gitbook.io/toolkit
10. NATO Strategic Communications Centre of Excellence. Robotrolling (регулярні звіти про діяльність ботмереж у соцмережах). Riga: NATO StratCom COE, 2017–2024. URL: https://stratcomcoe.org
11. The Great Hack. Directors: Karim Amer, Jehane Noujaim. Netflix, 2019.
12. The Social Dilemma. Director: Jeff Orlowski. Netflix, 2020.

9. ДОДАТКОВІ РЕСУРСИ

Онлайнові курси:

1. Інформаційна безпека. *Prometheus*. URL: https://prometheus.org.ua/prometheus-free/інформаційна-безпека/
2. Інформаційна гігієна під час війни. *Prometheus*. URL: https://prometheus.org.ua/prometheus-free/information-hygiene-during-war/
3. Інформаційні війни. *Prometheus*. URL: https://prometheus.org.ua/prometheus-free/information-wars/