

Рівненський державний гуманітарний університет
Кафедра політології та міжнародних відносин

Методичні рекомендації до вивчення курсу
«Інформаційні війни»
для здобувачів вищої освіти другого (магістерського) рівня
спеціальності С3 Міжнародні відносини

2025 – 2026 навчальний рік

Методичні рекомендації до вивчення курсу «Інформаційні війни» для здобувачів вищої освіти другого (магістерського) рівня спеціальності СЗ Міжнародні відносини. Рівне. РДГУ. 2025. 44 с.

Розробник: к.політ. наук, доц. кафедри політології та міжнародних відносин
Кундеус О. М.

Рецензенти:

Вівчар І.В. кандидат політичних наук, доцент кафедри політології та міжнародних відносин РДГУ.

Чернюк І.А. кандидат політичних наук, доцент кафедри суспільних наук Національного університету водного господарства та природокористування.

Методичні рекомендації до вивчення курсу допоможуть студентам більш глибоко зрозуміти та засвоїти зміст дисципліни «Інформаційні війни». Містять теми лекцій, плани практичних занять та літературу до них, теми для самостійної роботи, питання до контрольних робіт, термінологічний словник, список рекомендованої літератури.

Затверджено на засіданні кафедри політології та міжнародних відносин
Протокол від 29 травня 2025 № 7

Схвалено навчально-методичною комісією факультету історії, політології та міжнародних відносин
Протокол від 10 червня 2025 року № 6

©Кундеус О.М., 2025 рік

©РДГУ, 2025 рік

Мета та завдання навчальної дисципліни

Навчальна дисципліна «Інформаційні війни» є теоретичною основою сукупності знань та вмінь, що є підґрунтям становлення фахівця у галузі міжнародних відносин. Основною метою вивчення даної дисципліни є формування теоретичного мислення, оволодіння практичними навичками щодо безпеки інформаційних технологій та інформаційних ресурсів, захисту від шкідливого впливу інформації та інформаційної вразливості особистості, суспільства, цивілізації.

Завдання курсу. Актуальність процесів формування системної практики ведення інформаційних війн викликала необхідність комплексної підготовки майбутніх фахівців у галузі міжнародних відносин. Особливо гостро та актуально це питання постало в контексті подій на Півдні та Сході України.

У процесі вивчення курсу «Інформаційні війни» здобувачі вищої освіти повинні набути таких компетентностей:

Загальні компетентності:

ЗК2. Здатність вчитися і оволодівати сучасними знаннями.

ЗК3. Вміння виявляти, ставити та вирішувати проблеми.

ЗК5. Здатність генерувати нові ідеї (креативність).

Спеціальні (фахові) компетентності:

СК2. Здатність приймати обґрунтовані рішення щодо здійснення міжнародної та зовнішньополітичної діяльності.

СК4. Здатність аналізувати глобальні процеси та їх вплив на міжнародні та суспільні відносини, політичні та суспільні системи.

СК5. Здатність аналізувати та прогнозувати міжнародні відносини у різних контекстах, зокрема політичному, безпековому, правовому, економічному, суспільному, культурному та інформаційному.

Очікувані результати навчання

РН2. Критично осмислювати та аналізувати глобальні процеси та їх вплив на міжнародні відносини

РН4. Аналізувати та оцінювати проблеми міжнародної та національної безпеки, міжнародні та інтернаціоналізовані конфлікти, підходи, способи та

механізми забезпечення безпеки у міжнародному просторі та у зовнішній політиці держав.

РН6. Визначати, оцінювати та прогнозувати політичні, дипломатичні, безпекові, суспільні й інші ризики у сфері міжнародних відносин та глобального розвитку.

Програма навчальної дисципліни

Змістовий модуль 1. Теоретико-методологічні основи інформаційних війн.

Тема 1. Об'єкт та предмет курсу «Інформаційні війни». Актуальність, завдання, теоретичні засади.

Структура курсу. Рекомендовані джерела. Актуальність процесів формування системної практики ведення інформаційних війн. Основні завдання, які вирішує курс. Підходи до визначення сутності інформаційного протистояння/війни. Методології та методики ведення сучасних інформаційно-комунікаційних протистоянь. Актуальні напрямки дослідження інформаційних війн.

Тема 2. Війна як феномен міжнародної політики.

Війна як соціально-політичне явище: сутність, зміст, тенденції. Причини виникнення війн в історії людства. Класифікація війн. Еволюція війн.

Тема 3. Концептуальні засади інформаційної війни. ІВ як загроза національній та міжнародній безпеці.

Підходи до визначення сутності інформаційної війни. Поняття інформаційної війни. Характерні риси інформаційної війни. Види і підвиди інформаційної війни. Об'єкти інформаційної війни. Суб'єкти інформаційної війни. Інформаційні війни як компонент гібридних загроз. Аналіз впливу інформаційного тиску на національну безпеку, суверенітет, суспільну стабільність. Взаємозв'язок інформаційної політики та стратегій національної безпеки.

Змістовий модуль 2. Інструменти та технології інформаційного впливу.

Тема 4. Інформаційна зброя в інформаційному просторі.

Інформаційна зброя. Параметри інформаційної зброї. Класифікація інформаційної зброї. Інформаційна зброя і можливості нового етапу розвитку цивілізації. Боротьба за контроль і використання інформаційного простору. Характеристики інформаційної зброї. Відмінність звичайної зброї від інформаційної. Функції інформаційної зброї. Переваги і недоліки листівок як засобу інформаційно-психологічного впливу. Особливості використання газет і брошур в інформаційних операціях. Практика використання друкованих засобів в сучасних інформаційних операціях. Переваги і недоліки радіо як засобу інформаційної війни. Види радіопередач. Вимоги до радіоповідомлень. Переваги і недоліки телебачення в інформаційних операціях. Приклади використання радіо і ТБ в інформаційних війнах сучасності. Характеристика мережі Інтернет як середовища для інформаційного протиборства. Напрями використання мережі Інтернет в інформаційних війнах. Специфіка використання веб-сайтів, е-пошти і соціальних медіа в інформаційному протиборстві.

Тема 5. Психологічні операції як ключовий елемент інформаційного протиборства.

Історія питання. Базові операції психологічних воєн. Роль і статус психологічних операцій в сучасному інформаційному протиборстві. Історична ретроспектива психологічних операцій XX століття. Психологічні операції як ключовий елемент інформаційного протиборства. Види психологічного впливу.

Тема 6. Пропаганда як форма проведення психологічних операцій.

Пропаганда як форма проведення психологічних операцій. Принципи і правила пропагандистського впливу. Пропагандистські методи в інформаційних війнах. Переконавання і навіювання в психологічних операціях. Приклади дезінформаційних заходів в сучасних інформаційних війнах. Класифікація чуток як засобу інформаційно-психологічного впливу. Практика використання чуток в інформаційному протиборстві.

Тема 7. Креативні технології в інформаційній боротьбі: меми, візуальний контент, соціальні мережі.

Креатив як зброя: створення і поширення інформаційних мемів, інфографіки, емоційно-зарядженого контенту. Роль мемів у формуванні інформаційного середовища, їх використання у міжнародних інформаційних конфліктах. Візуальна пропаганда. Інформаційні стратегії в соціальних мережах. Візуальні наративи в умовах гібридного протистояння. Вплив гумору, сатири, візуального символізму на суспільну думку.

Змістовий модуль 3. Міжнародна практика інформаційного протиборства.

Тема 8. Інформаційні війни в історії людства.

Інформаційно-психологічне протиборство у стародавньому світі та в епоху Середньовіччя. Військове мистецтво Стародавнього Китаю, Стародавньої Греції. Монгольська імперія. Тридцятирічна війна (1618–1648). Релігійні ідеї в інформаційно-психологічному забезпеченні війн часів Середньовіччя. Інформаційно-психологічне протиборство у воєнних конфліктах XIX ст. Наполеонівські війни.

Тема 9. Інформаційні війни XX - поч.XXI ст.

Інформаційно-психологічне протиборство під час Першої світової війни. Інформаційно-психологічне протиборство в міжвоєнний період. Інформаційно-психологічне протиборство в роки Другої світової війни. Інформаційно-психологічне протиборство часів «холодної війни».

Змістовий модуль 4. Інформаційні війни у глобальному контексті.

Тема 10. Російсько-українська інформаційна війна: стратегії, наративи, вплив.

Основні методи інформаційної агресії проти України. Дезінформування та маніпулювання. Пропаганда. Диверсифікація громадської думки. Психологічний та психотропний тиск. Поширення чуток. Інформаційні війни епохи незалежності. Механізми протидії інформаційній війні Росії проти України. Шляхи вдосконалення системи забезпечення національної безпеки України в інформаційній сфері.

Тема 11. Інформаційні кампанії США, ЄС та Китаю на міжнародній арені.

Особливості та механізми інформаційних кампаній трьох ключових гравців світової політики: США, Китаю та Європейського Союзу. Цілі, інструменти, канали поширення інформації, а також результати та виклики, які виникають у процесі їх реалізації. М'яка сила, цифрова дипломатія, інформаційне просування інтересів.

Змістовий модуль 5. Протидія інформаційним загрозам та інформаційна безпека.

Тема 12. Інформаційна безпека як складова зовнішньої політики держави.

Визначення поняття інформаційної безпеки у міжнародному праві та зовнішньополітичній практиці. Місце інформаційної безпеки у стратегіях національної безпеки та зовнішньополітичних доктринах провідних держав. Роль дипломатії, публічної дипломатії та стратегічних комунікацій у забезпеченні інформаційної безпеки. Вплив інформаційної безпеки на формування міжнародного іміджу та реалізацію геополітичних стратегій. Політика інформаційного захисту в системі національних інтересів.

Тема 13. Механізми виявлення та нейтралізації інформаційних атак.

Визначення інформаційної атаки: види, цілі, технології. Джерела інформаційних атак: державні та недержавні актори. Алгоритми та платформи для виявлення фейкової інформації (OSINT, фактчекінг). Ідентифікація бот-мереж, скоординованої неавтентичної поведінки (CIB). Моніторинг медіаполя та аналіз інформаційних хвиль. Механізми державної, корпоративної та громадської нейтралізації атак. Реактивна і проактивна комунікація як засіб протидії.

Структура навчальної дисципліни

Назви змістових модулів і тем	Кількість годин				
	усього	у тому числі			
		лек	пр.	лаб	інд
ЗМІСТОВИЙ МОДУЛЬ 1.	1.	Теоретико-методологічні основи			

інформаційних війн.						
Тема 1. Об'єкт та предмет курсу «Інформаційні війни». Актуальність, завдання, теоретичні засади.	12	2	2	—	—	8
Тема 2. Війна як феномен міжнародної політики.	12	2	2	—	—	8
Тема 3. Концептуальні засади інформаційної війни. ІВ як загроза національній та міжнародній безпеці.	12	2	2	—	—	8
ЗМІСТОВИЙ МОДУЛЬ 2. Інструменти та технології інформаційного впливу.						
Тема 4. Інформаційна зброя в інформаційному просторі.	12	2	2	—	—	8
Тема 5. Психологічні операції як ключовий елемент інформаційного протиборства.	12	2	2	0	0	8
Тема 6. Пропаганда як форма проведення психологічних операцій.	12	2	2			8
Тема 7. Креативні технології в інформаційній боротьбі: меми, візуальний контент, соціальні мережі.	12	2	2			8
ЗМІСТОВИЙ МОДУЛЬ 3. Міжнародна практика інформаційного протиборства.						

Тема 8. Інформаційні війни в історії людства	10	2	1	–	–	7
Тема 9. Інформаційні війни XX - поч.XXI ст.	10	2	1	–	–	7
ЗМІСТОВИЙ МОДУЛЬ 4. Інформаційні війни у міжнародному контексті.						
Тема 10. Російсько-українська інформаційна війна: стратегії, наративи, вплив.	12	2	2			8
Тема 11. Інформаційні кампанії США, ЄС та Китаю на міжнародній арені.	11	2	2			7
ЗМІСТОВИЙ МОДУЛЬ 5. Протидія інформаційним загрозам та інформаційна безпека.						
Тема 12. Інформаційна безпека як складова зовнішньої політики держави.	12	2	2			8
Тема 13. Механізми виявлення та нейтралізації інформаційних атак.	11	2	2			7
Усього годин	150	26	24	0	0	100

Методичні рекомендації з підготовки практичних занять.

Мета семінарських занять – поглиблення та закріплення знань, отриманих на лекціях і під час самостійного вивчення окремих тем курсу. Як правило, на семінар виносяться 3–4 питання; їх розглядають як у традиційній формі, так і у вигляді дискусії, розгорнутої бесіди, конференції, «круглого столу»,

особливо якщо обговорюються проблемні питання. Опитування студентів на семінарі проходить як за бажанням студента, так і за викликом викладача. Крім основних виступів студентів на семінарі, викладач оцінює також істотні доповнення до викладеної проблеми. На семінарських заняттях можуть обговорюватися повідомлення, доповіді та реферати.

У кінці заняття викладач підводить підсумки роботи, оцінює виступи і доповнення кожного студента, акцентуючи увагу на найбільш вдалих відповідях, недоліках у висвітленні теми. Крім цього, студенти отримують завдання щодо підготовки до наступного семінарського заняття. Оцінки, одержані на семінарі, обов'язково враховуються при рейтинго-модульній системі контролю знань.

Готуючись до семінарського заняття, студент повинен опрацювати рекомендовані до даної теми джерела та літературу, продумати відповіді на кожне питання, скласти план і стислі тези свого виступу. Важливе значення у підготовці до семінару мають консультації викладачів, час і місце проведення яких доводиться до відома студентів. Готуватися до семінарського заняття необхідно заздалегідь. Всебічна та ґрунтовна підготовка – важлива передумова створення творчої атмосфери при обговоренні передбачених планом семінару питань, змістовних виступів і доповнень. На семінарі студенти повинні доповнювати свої записи новим матеріалом з виступів своїх товаришів та викладача.

Семінарські заняття базуються на самостійній роботі студентів, яка є однією з основних форм навчального процесу. Лише самостійна робота в комплексі з іншими формами навчання забезпечує глибоке вивчення та всебічне засвоєння студентами матеріалу, оволодіння методами наукового мислення, виховання у них творчих, аналітичних підходів до вивчення дисципліни. Форми самостійної роботи студентів можуть бути різноманітними: вивчення і конспектування документів та інших історичних джерел, навчальної та навчально-методичної літератури, монографій і наукових статей, написання тематичних повідомлень, доповідей, рефератів. Основна ділянка самостійної роботи – уважне читання і конспектування

передбачених до семінарського заняття основних джерел та літератури. Це обов'язкова вимога при вивченні інформаційної безпеки, один з головних елементів модульно-рейтингової системи оцінки знань студентів

Теми практичних занять

Тема 1. Об'єкт та предмет курсу «Інформаційні війни». Актуальність, завдання, теоретичні засади.

1. Об'єкт та предмет дисципліни.
2. Основні завдання курсу Інформаційні війни.
3. Методи ведення сучасних інформаційних війн.

Література.

1. Гамова І. В. Інформаційні війни : підручник / І. В. Гамова. Київ : Держ. торг.-екон. ун-т, 2022. 184 с.
2. Інформаційна війна і національна безпека: монографія / П. П. Ткачук [та ін.]. Львів: Акад. сухопут. військ, 2015. 264 с.
3. Інформаційні війни: монографія / Д. В. Кіслов. Київ. Нац. торг.-екон. ун-т. Київ. 2013. 300 с.
4. Худолій А. О. Інформаційна війна 2014-2022 рр. : монографія. Острог : Видавництво Національного університету «Острозька академія», 2022. 208 с.
5. Почепцов Г. Сучасні інформаційні війни. Вид. 2-ге, допов. Київ: КиєвоМорил. акад., 2016. 502 с.

Тема 2. Війна як феномен міжнародної політики.

1. Війна як соціально-політичне явище: сутність, зміст, тенденції.
2. Причини виникнення війн в історії людства.
3. Класифікація війн.
4. Еволюція війн.

Література.

1. Гамова І. В. Інформаційні війни : підручник / І. В. Гамова. Київ : Держ. торг.-екон. ун-т, 2022. 184 с.
2. Інформаційні війни: монографія / Д. В. Кіслов. Київ. Нац. торг.-екон. ун-т. Київ. 2013. 300 с.

3. Опорний конспект лекцій з дисципліни «Інформаційні війни» для студентів спеціальності 7.030404 «Міжнародна інформація» Б.М.Юськів. Рівне: РІС КСУ, 2003. 55 с.
4. Почепцов Г. Сучасні інформаційні війни. Вид. 2-ге, допов. Київ: КиєвоМорил. акад., 2016. 502 с.

Тема 3. Концептуальні засади інформаційної війни. ІВ як загроза національній та міжнародній безпеці.

1. Підходи до визначення сутності інформаційної війни.
2. Поняття інформаційної війни. Характерні риси інформаційної війни.
3. Об'єкти та суб'єкти інформаційної війни.
4. Інформаційні війни як компонент гібридних загроз.
5. Аналіз впливу інформаційного тиску на національну безпеку, суверенітет, суспільну стабільність.
6. Взаємозв'язок інформаційної політики та стратегій національної безпеки.

Література.

1. Гамова І. В. Інформаційні війни : підручник / І. В. Гамова. Київ : Держ. торг.-екон. ун-т, 2022. 184 с.
2. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник / за заг. ред. В. О. Жадька. Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.
3. Горбулін В. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. Київ: НІСД, 2017. 496 с.
4. Інформаційна війна і національна безпека: монографія / П. П. Ткачук [та ін.]. Львів: Акад. сухопут. військ, 2015. 264 с.
5. Інформаційні війни: монографія / Д. В. Кіслов. Київ. Нац. торг.-екон. ун-т. Київ. 2013. 300 с.
6. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської. Київ: НІСД, 2016. 109 с

7. Почепцов Г. Сучасні інформаційні війни. Вид. 2-ге, допов. Київ: КиєвоМогилян. акад., 2016. 502 с.
8. Національна безпека в умовах інформаційних та гібридних війн: монографія за заг. ред. В. Куйбіди і В. Бебика; Нац. акад. держ. упр. при Президентові України, Ред. пол.-укр. журн. «Соц.-гуманітар. Науки». Київ: НАДУ, 2019. 380 с.

Тема 4. Інформаційна зброя в інформаційному просторі.

1. Інформаційна зброя та її параметри.
2. Класифікація інформаційної зброї.
3. Функції інформаційної зброї.
4. Характеристика мережі Інтернет як середовища для інформаційного протиборотства.
5. Напрями використання мережі Інтернет в інформаційних війнах.

Література.

1. Історія інформаційно-психологічного протиборотства: підруч. / за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. Київ: Наук.-вид. відділ НА СБ України, 2012. 212 с.
2. Інформаційно-психологічне протиборотство (еволюція та сучасність): монографія / Я. М. Жарков [та ін.]; Військ. ін-т Київ. нац. ун-ту ім. Т. Г. Шевченка. Київ: Віпол, 2013. 247 с.
3. Інформаційні війни у соціальних он-лайн-мережах: [монографія] / Курбан О. В. ; Київ. ун-т ім. Бориса Грінченка. Київ: Київ. ун-т ім. Бориса Грінченка, 2017. 392 с.
4. Почепцов Г. Сучасні інформаційні війни. Вид. 2-ге, допов. Київ: КиєвоМогилян. акад., 2016. 502 с.
5. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник / О.В.Курбан. Київ: ВІКНУ, 2016. 286 с.

Тема 5. Психологічні операції як ключовий елемент інформаційного протиборотства.

1. Роль і статус психологічних операцій в сучасному інформаційному протиборстві.
2. Історична ретроспектива психологічних операцій ХХ століття.
3. Психологічні операції як ключовий елемент інформаційного протиборства.
4. Види психологічного впливу.

Література.

1. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах / П. С. Прибутко, І. Б. Лук'янець. Київ: Поливода А. В., 2007. 252 с.
2. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін Рада нац. безпеки і оборони України; Ін-т проблем нац. безпеки. Київ: Інтертехнологія, 2009. 164 с.
3. Історія інформаційно-психологічного протиборства: підруч. / за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. Київ: Наук.-вид. відділ НА СБ України, 2012. 212 с.
4. Інформаційно-психологічне протиборство (еволюція та сучасність): монографія / Я. М. Жарков [та ін.]; Військ. ін-т Київ. нац. ун-ту ім. Т. Г. Шевченка. Київ: Віпол, 2013. 247 с.
5. Сенси і війни: Україна і Росія в інформаційній і сенсиовій війнах. Георгій Почепцов; пер. з рос. Тамари Гуменюк. Київ: Києво-Могила акад., 2016. 312 с.

Тема 6. Пропаганда як форма проведення психологічних операцій.

1. Пропаганда як форма проведення психологічних операцій.
2. Принципи і правила пропагандистського впливу.
3. Пропагандистські методи в інформаційних війнах.
4. Переконавання і навіювання в психологічних операціях.

Література.

1. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської. Київ: НІСД, 2016. 109 с
2. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах / П. С. Прибутко, І. Б. Лук'янець. Київ: Поливода А. В., 2007. 252 с.
3. Опорний конспект лекцій з дисципліни «Інформаційні війни» для студентів спеціальності 7.030404 «Міжнародна інформація» Б.М.Юськів. Рівне: РІС КСУ, 2003. 55 с.
4. Сенси і війни: Україна і Росія в інформаційній і смисловій війнах. Георгій Почепцов; пер. з рос. Тамари Гуменюк. Київ: Києво-Могилянська акад., 2016. 312 с.
5. Худолій А. О. Інформаційна війна 2014-2022 рр. : монографія. Острогозьк : Видавництво Національного університету «Острогозька академія», 2022. 208 с.

Тема 7. Інформаційні війни в історії людства.

1. Інформаційно-психологічне протиборство у стародавньому світі.
2. Військове мистецтво Стародавнього Китаю, Стародавньої Греції.
3. Релігійні ідеї в інформаційно-психологічному забезпеченні війн часів Середньовіччя.
4. Інформаційно-психологічне протиборство у воєнних конфліктах ХІХ ст.

Література.

1. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник / за заг. ред. В. О. Жадька. Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.
2. Інформаційно-психологічне протиборство (еволюція та сучасність): монографія / Я. М. Жарков [та ін.]; Військ. ін-т Київ. нац. ун-ту ім. Т. Г. Шевченка. Київ: Віпол, 2013. 247 с.

3. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник / О.В.Курбан. Київ: ВІКНУ, 2016. 286 с.
4. Опорний конспект лекцій з дисципліни «Інформаційні війни» для студентів спеціальності 7.030404 «Міжнародна інформація» Б.М.Юськів. Рівне: РІС КСУ, 2003. 55 с.
5. Сенси і війни: Україна і Росія в інформаційній і сенсиовій війнах. Георгій Почепцов; пер. з рос. Тамари Гуменюк. Київ: Києво-Могилянська акад., 2016. 312 с.

Тема 8. Інформаційні війни ХХ - поч.ХХІ ст.

1. Інформаційно-психологічне протиборство під час Першої світової війни.
2. Інформаційно-психологічне протиборство в міжвоєнний період.
3. Інформаційно-психологічне протиборство в роки Другої світової війни.
4. Інформаційно-психологічне протиборство часів «холодної війни».

Література.

1. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник / за заг. ред. В. О. Жадька. Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.
2. Інформаційно-психологічне протиборство (еволюція та сучасність): монографія / Я. М. Жарков [та ін.]; Військ. ін-т Київ. нац. ун-ту ім. Т. Г. Шевченка. Київ: Віпол, 2013. 247 с.
3. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник / О.В.Курбан. Київ: ВІКНУ, 2016. 286 с.
4. Опорний конспект лекцій з дисципліни «Інформаційні війни» для студентів спеціальності 7.030404 «Міжнародна інформація» Б.М.Юськів. Рівне: РІС КСУ, 2003. 55 с.
5. Сенси і війни: Україна і Росія в інформаційній і сенсиовій війнах. Георгій Почепцов; пер. з рос. Тамари Гуменюк. Київ: Києво-Могилянська акад., 2016. 312 с.

Тема 9. Російсько-українська інформаційна війна: стратегії, наративи, вплив.

1. Основні методи інформаційної агресії проти України.
2. Дезінформування та маніпулювання. Пропаганда.
3. Інформаційні війни епохи незалежності.
4. Механізми протидії інформаційній війні Росії проти України.
5. Шляхи вдосконалення системи забезпечення національної безпеки України в інформаційній сфері.

Література.

1. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник / за заг. ред. В. О. Жадька. Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.
2. Горбулін В. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. Київ: НІСД, 2017. 496 с.
3. Інформаційна війна і національна безпека: монографія / П. П. Ткачук [та ін.]. Львів: Акад. сухопут. військ, 2015. 264 с.
4. Сенси і війни: Україна і Росія в інформаційній і смисловій війнах. Георгій Почепцов; пер. з рос. Тамари Гуменюк. Київ: Києво-Могилянська акад., 2016. 312 с.
5. Худолій А. О. Інформаційна війна 2014-2022 рр. : монографія. Острогозьк : Видавництво Національного університету «Острозька академія», 2022. 208 с.
6. Національна безпека в умовах інформаційних та гібридних війн: монографія за заг. ред. В. Куйбіди і В. Бебика; Нац. акад. держ. упр. при Президенті України, Ред. пол.-укр. журн. «Соц.-гуманітар. Науки». Київ: НАДУ, 2019. 380 с.

Тема 10. Інформаційні кампанії США, ЄС та Китаю на міжнародній арені.

1. Особливості та механізми інформаційних кампаній трьох ключових гравців світової політики: США, Китаю та Європейського Союзу.
2. Цілі, інструменти, канали поширення інформації.

3. М'яка сила, цифрова дипломатія, інформаційне просування інтересів.

Література.

1. Гамова І. В. Інформаційні війни : підручник / І. В. Гамова. Київ : Держ. торг.-екон. ун-т, 2022. 184 с.
2. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник / за заг. ред. В. О. Жадька. Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.
3. Інформаційні війни у соціальних он-лайн-мережах: [монографія] / Курбан О. В. ; Київ. ун-т ім. Бориса Грінченка. Київ: Київ. ун-т ім. Бориса Грінченка, 2017. 392 с.
4. Почепцов Г. Сучасні інформаційні війни. Вид. 2-ге, допов. Київ: КиєвоМогил. акад., 2016. 502 с.
5. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник / О.В.Курбан. Київ: ВІКНУ, 2016. 286 с.
6. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін Рада нац. безпеки і оборони України; Ін-т проблем нац. безпеки. Київ: Інтертехнологія, 2009. 164 с

Тема 11. Інформаційна безпека як складова зовнішньої політики держави.

1. Визначення поняття інформаційної безпеки.
2. Місце інформаційної безпеки у стратегіях національної безпеки та зовнішньополітичних доктринах провідних держав.
3. Роль дипломатії, публічної дипломатії та стратегічних комунікацій у забезпеченні інформаційної безпеки.
4. Вплив інформаційної безпеки на формування міжнародного іміджу та реалізацію геополітичних стратегій.
5. Політика інформаційного захисту в системі національних інтересів.

Література.

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: ДУТ. 2015. 288 с.
2. Жарков Я.М., Дзюба М.Т., Замаруєва І.В., ін. Інформаційна безпека особистості, суспільства, держави: Підручник. Київ: Видавничо-поліграфічний центр "Київський університет", 2008. 274 с.
3. Інформаційна безпека. Підручник / В. В. Остроухов, М. М. Присяжнюк, О. І. Фармагей, М. М. Чеховська та ін.; під ред. В. В. Остроухова. Київ: Видавництво Ліра-К, 2021. 412 с.
4. Інформаційна безпека держави: навч. посіб. для студ. / В.І. Гур'єв, Д.Б. Мехед, Ю.М. Ткач, І.В. Фірсова. Ніжин: ФОП Лук'яненко В.В. ТПК «Орхідея», 2018. 166 с.
5. Кавун С. В. Інформаційна безпека. Навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. Харків: Вид. ХНЕУ, 2000. 352 с.
6. Кормич Б. Інформаційна безпека: організаційно-правові основи : навч. посіб. / Кормич Б. Київ: Кондор, 2004. 384 с.
7. Мужанова Т.М. Інформаційна безпека держави: навчальний посібник. Київ: Державний університет телекомунікацій, 2021. 201 с.
8. Остроухов В.В. Інформаційна безпека (соціально-правові аспекти). Підручник / Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін. ; за заг. ред. Є.Д.Скулиша. Київ: КНТ. 2010. 776 с.

Тема 12. Механізми виявлення та нейтралізації інформаційних атак.

1. Визначення інформаційної атаки: види, цілі, технології.
2. Джерела інформаційних атак: державні та недержавні актори.
3. Алгоритми та платформи для виявлення фейкової інформації (OSINT, фактчекінг).
4. Ідентифікація бот-мереж, скоординованої неавтентичної поведінки (CIB).
5. Механізми державної, корпоративної та громадської нейтралізації атак.
6. Реактивна і проактивна комунікація як засіб протидії.

Література.

1. Гамова І. В. Інформаційні війни : підручник / І. В. Гамова. Київ : Держ. торг.-екон. ун-т, 2022. 184 с.
2. Інформаційна війна і національна безпека: монографія / П. П. Ткачук [та ін.]. Львів: Акад. сухопут. військ, 2015. 264 с.
3. Інформаційні війни: монографія / Д. В. Кіслов. Київ. Нац. торг.-екон. ун-т. Київ. 2013. 300 с.
4. Інформаційні війни у соціальних он-лайн-мережах: [монографія] / Курбан О. В. ; Київ. ун-т ім. Бориса Грінченка. Київ: Київ. ун-т ім. Бориса Грінченка, 2017. 392 с.
5. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської. Київ: НІСД, 2016. 109 с
6. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах / П. С. Прибутко, І. Б. Лук'янець. Київ: Поливода А. В., 2007. 252 с.
7. Історія інформаційно-психологічного протиборства: підруч. / за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. Київ: Наук.-вид. відділ НА СБ України, 2012. 212 с.

Самостійна робота студентів.

1. Мета й завдання самостійної роботи студентів

- а) закріплення у студентів умінь і навичок роботи з науковою літературою (конспектування, виписування тез, загальне ознайомлення тощо);
- б) закріплення у студентів володіння методикою укладання словника, креслення схем і таблиць;
- в) краще усвідомлення та запам'ятовування матеріалу під час виконання завдань для самостійної роботи;
- г) систематизування знань під час укладання словника.

2. Форми організації самостійної роботи

1. Забезпечити студентів необхідними навчально-методичними матеріалами (підручниками й посібниками, фаховими виданнями, адресами в Інтернеті, текстами лекцій тощо).
2. Чітко визначити зміст і методи виконання завдань для самостійної роботи: – подати чіткий список завдань для самостійного опрацювання

відповідно до кожної теми; – до кожного завдання обов’язково вказати джерело й конкретні сторінки, що потрібно опрацювати; – зазначити методи виконання самостійної роботи для кожного конкретного завдання (конспектування, тези, виписки, загальне ознайомлення тощо); – подати чіткий список термінів відповідно до кожної теми із зазначенням джерела, звідки можна виписати дефініцію даних понять.

3. Організувати системний контроль за виконанням студентами завдань для самостійного опрацювання.

3.1. Вхідний контроль: подати питання для повторення положень основних законів, які формують сучасне правове поле інформаційної діяльності.

3.2. Поточний контроль: а) перевіряти виконання студентами індивідуальних завдань; б) перевіряти виконання студентами завдань для самостійного опрацювання; в) перевіряти ведення словника.

3.3. Підсумковий контроль: розробити питання для підсумкового колоквиуму, що проводиться наприкінці вивчення курсу.

Методичні рекомендації до самостійної роботи.

Курс «Інформаційні війни» вивчається протягом одного семестру. Навчально-тематичним планом передбачена самостійна робота з найбільш актуальних і складних тем курсу. На самостійну роботу виносяться основні та додаткові питання і завдання, передбачені запропонованими планами, і вони проводяться під керівництвом викладачів з використанням різних форм та методів контролю знань студентів: тестування, опитування, вільна дискусія, обговорення реферативних повідомлень, перевірка робочих зошитів, глосарію.

При виконанні самостійної роботи студенти можуть зіткнутися з певними труднощами, пов’язаними, передусім, з браком джерел з дисципліни, що вивчається. У зв’язку з цим студенти мають звернути особливу увагу на: 1) ретельне конспектування лекцій; 2) самостійне вивчення наукових праць, перелік яких дається на лекціях, а також міститься у робочій програмі в розділі «Література». Ураховуючи зазначене, ведення робочого зошиту є доцільним елементом підготовки до занять.

Крім цього, для формування понятійного апарату студентам рекомендовано вести власний тезаурус, в якому відображатимуться ключові терміни, що відповідають конкретній темі. Перелік цих термінів не є жорстко визначеним і залежить від творчого підходу кожного студента, водночас їхній перелік становить базовий мінімум і міститься наприкінці даної програми у розділі «Термінологічний мінімум». За відсутності робочого зошиту із відпрацьованими темами і тезаурусу студенти не зможуть успішно оволодіти даним предметом.

Студенту, під час індивідуальної співбесіди, з обговорення реферату, при висвітленні питань теми дозволяється користуватися робочим зошитом, власним тезаурусом. Студенту можуть ставитися додаткові запитання.

Наприкінці обговорення рефератів, дискусії тощо, викладач оцінює знання студентів і рівень підготовки групи в цілому, наголошує на питаннях, які потребуються більш детального вивчення під час подальшої самостійної роботи.

Завершується вивчення курсу «Інформаційні війни» складанням іспиту.

Перелік тем для самостійної роботи

№ з/п	Назва теми	Кількість годин
1	Історичні приклади інформаційних війн: від античності до XX століття.	7
2	Російська дезінформація у міжнародному просторі: методи, наративи, канали.	7
3	Інформаційні війни у кіберпросторі: атаки на інфраструктуру та елементи психологічного тиску.	7
4	Фейки як інструмент політичного впливу: анатомія дезінформаційної кампанії.	7
5	Роль соціальних мереж у розгортанні інформаційних операцій.	7
6	Мемна культура як зброя інформаційної війни.	6

7	Публічна дипломатія та пропаганда: межа між легітимною комунікацією та маніпуляцією.	7
8	Інформаційна безпека України: виклики та стратегічні відповіді.	7
9	Західні механізми протидії інформаційним атакам (NATO, EUvsDisinfo, StratCom COE).	7
10	Інформаційні кампанії Китаю: “м’яка сила”, технологічний контроль та глобальні наративи.	7
11	Інформаційні війни під час пандемії COVID-19: приклади і наслідки.	6
12	Міжнародне право та регулювання інформаційної безпеки: сучасний стан і прогалини.	6
13	Гібридна війна як багатовимірне явище: місце інформаційного компонента.	7
14	Етика і свобода слова в умовах протидії дезінформації.	6
15	Аналітика інформаційного простору: як працюють медіа-моніторинг і OSINT-дослідження.	6
	Разом	100

Методичні рекомендації для виконання контрольних робіт.

Навчальний процес в РДГУ передбачає різні форми індивідуальної роботи слухачів, однією з яких є виконання контрольних робіт. Основне завдання контрольної роботи - це формування власної думки слухачів з теоретичних та практичних питань, які розглядаються, та внесення ними пропозицій щодо їх вирішення. Підготовка контрольної роботи повинна розпочатися з вивчення методичних рекомендацій за темою та інших публікацій з питань, що досліджуються. Робота повинна бути виконана слухачами самостійно та належним чином оформлена. Вимоги до оформлення. Контрольна робота виконується і подається слухачем на перевірку викладачеві як в надрукованому вигляді так і допускається її представлення у рукописному варіанті. Сторінки мають бути пронумерованими. Контрольна робота має бути

написана українською мовою. Першим листом контрольної роботи є титульний лист. Планом контрольної роботи є завдання за певним варіантом. В контрольній роботі обов'язково перелічуються всі використані джерела наукової літератури та нормативні акти. Література і нормативні акти, що цитуються, повинні бути оформлені у вигляді загального списку у порядку цитування або за абеткою. Цінним додатком до роботи є таблиці та схеми. Таблиці і схеми відокремлюються від основного тексту пустими рядками. Основні висновки, пропозиції та рекомендації необхідно оформляти в заключній частині роботи. Контрольна робота в обов'язковому порядку перевіряється викладачем. Контрольна робота оцінюється за змістом, ступенем самостійності виконання, вмінням під час захисту обґрунтувати основні положення роботи та зроблені в ній висновки.

Питання на контрольну роботу.

Варіант 1.

1. Основи теорії інформаційної війни.
2. Поняття психологічної війни і спеціальних інформаційних операцій

Варіант 2.

1. Інформаційна війна та інформаційна боротьба: основні поняття.
2. Інформаційне суспільство і відкритість влади.

Варіант 3.

1. Форми та способи ведення інформаційної боротьби.
2. Державна інформаційна політика України.

Варіант 4.

1. Психологічна і кібернетична війна як складові інформаційної війни.
2. Пропагандистські технології і сценарії психологічних операцій.

Проблеми захисту від інформаційних операцій і контрпропаганда.

Варіант 5.

1. Інформаційна зброя і технології її використання.
2. Сучасний стан інформаційної сфери України.

Варіант 6.

1. Психологічні війни і методи їх ведення.

2. Комунікативні складові інформаційної війни.

Варіант 7.

1. Об'єкти впливу і класифікація спеціальних інформаційних операцій.
2. Основні проблеми правового регулювання мережі Інтернет.

Варіант 8.

1. Методи дослідження спеціальних інформаційних операцій.
2. Основи законодавства України в інформаційній сфері.

Варіант 9.

1. Система захисту інформаційного простору від спеціальних інформаційних операцій.
2. Закони України щодо регулювання різних аспектів інформаційної діяльності.

Варіант 10.

1. Контрпропаганда в інформаційних війнах.
2. Інформаційні війни у структурі сучасних цивілізацій.

Методи навчання.

МН1 –словесний метод (лекція, дискусія, співбесіда тощо);

МН2 –практичний метод (лабораторні та практичні заняття);

МН4 – робота з навчально-методичною літературою (конспектування, тезування, анотування, рецензування, складання реферату);

МН6 –самостійна робота (розв'язання завдань);

МН7 – індивідуальна науково-дослідна робота здобувачів вищої освіти.

Методи оцінювання.

МО1 –екзамени;

МО2 –усне або письмове опитування,

МО6 – реферати, есе;

МО7 – презентації результатів виконаних завдань та досліджень;

МО8 – презентації та виступи на наукових заходах;

МО9 – захист лабораторних і практичних робіт;

Засоби діагностики результатів навчання:

- экзамены;

- реферати, есе;
- презентації результатів виконаних завдань та досліджень;
- інші види.

Види та методи навчання і оцінювання

Код компетентності (згідно ОПП)	Назва компетентності	Код програмного результату навчання	Назва програмного результату навчання	Методи навчання	Методи оцінювання результатів навчання
ЗК 02	Здатність вчитися і оволодівати сучасними знаннями.	РН2.	Критично осмислювати та аналізувати глобальні процеси та їх вплив	МН 1, МН4, МН5, МН 6, МН7	МО1, МО2, МО3, МО4, МО6, МО7.
ЗК 03	Вміння виявляти, ставити та вирішувати проблеми.	РН4.	Аналізувати та оцінювати проблеми міжнародної та національної безпеки, міжнародні та інтернаціоналізовані конфлікти, підходи, способи та		
ЗК 05					
СК 02	Здатність генерувати нові ідеї (креативність).				
	Здатність приймати обґрунтовані рішення щодо				

СК 04	здійснення міжнародної та зовнішньополітичної діяльності.		механізми забезпечення безпеки у міжнародному просторі та у зовнішній політиці держав.		
СК 05	Здатність аналізувати глобальні процеси та їх вплив на міжнародні та суспільні відносини, політичні та суспільні системи Здатність аналізувати та прогнозувати міжнародні відносини у різних контекстах, зокрема політичному, безпековому, правовому, економічному, суспільному, культурному та	РН6	Визначати, оцінювати та прогнозувати політичні, дипломатичні, безпекові, суспільні й інші ризики у сфері міжнародних відносин та глобального розвитку.		

	інформаційному.				
--	-----------------	--	--	--	--

Критерії оцінювання результатів навчання.

Система та критерії оцінювання у Рівненському державному гуманітарному університеті

Критерії оцінювання. Еквівалент оцінки в балах для кожної окремої теми може бути різний, загальну суму балів за тему визначено в розподілі балів, які отримують здобувачі вищої освіти при вивченні дисципліни.

Результат освітньої діяльності здобувача вищої освіти оцінюється згідно Положення про оцінювання знань і умінь здобувачів вищої освіти РДГУ за такими рівнями та критеріями:

Суми балів за 100-бальною шкалою	Оцінка в ЄКТС	Значення оцінки ЄКТС	Критерії оцінювання	Рівень компетентності	Оцінка за національною шкалою	
					екзамени	залік
90-100	A	Відмінно	здобувач вищої освіти виявляє особливі творчі здібності, вміє самостійно здобувати знання, без допомоги викладача знаходить і опрацьовує необхідну інформацію, вміє використовувати набуті знання і вміння для прийняття рішень у нестандартних ситуаціях, переконливо аргументує відповіді, самостійно розкриває власні здібності	Високий (творчий)	Відмінно	Зараховано
82-89	B	Дуже	здобувач вищої освіти			

		добре	вільно володіє теоретичним матеріалом, застосовує його на практиці, вільно розв'язує вправи і задачі у стандартних ситуаціях, самостійно виправляє допущені помилки, кількість яких незначна.	Достатній (конструктивно-варіативний)	Добре	Зараховано
74-81	С	Добре	здобувач вищої освіти вміє зіставляти, узагальнювати, систематизувати інформацію під керівництвом викладача, загалом самостійно застосовувати її на практиці; контролювати власну діяльність; виправляти помилки, з-поміж яких є суттєві, добирати аргументи для підтвердження думок			
64-73	D	Задовільно	здобувач вищої освіти відтворює значну частину теоретичного матеріалу, виявляє знання і розуміння основних положень, за допомогою викладача може аналізувати навчальний			

			матеріал, виправляти помилки, з-поміж яких є значна кількість суттєвих.	Середній	Задовільно	Зараховано
60-63	Е	Достатньо	здобувач вищої освіти володіє навчальним матеріалом на рівні, вищому за початковий, значну частину його відтворює на репродуктивному рівні	(репродуктивний)		
35-59	FX	Незадовільно з можливістю повторного складання семестрового контролю	здобувач вищої освіти володіє матеріалом на рівні окремих фрагментів, що становлять незначну частину навчального матеріалу	Низький (рецептивно-продуктивний)	Незадовільно	Незараховано
1-34	F	незадовільно з обов'язковим повторним вивченням	здобувач вищої освіти володіє матеріалом на рівні елементарного розпізнання і відтворення окремих фактів, елементів, об'єктів	Низький (рецептивно-продуктивний)	Незадовільно	Незараховано

		дисципліни				
--	--	------------	--	--	--	--

14. Розподіл балів, які отримують здобувачі вищої освіти

Поточне тестування та самостійна робота													Підсумковий тест (екзамен)	Сума
ЗМ 1			ЗМ 2				ЗМ 3		ЗМ 4		ЗМ			
T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13		
4	5	4	5	5	5	4	5	5	4	5	4	5	40	100

Перелік питань які виносяться на екзамен

1. Визначення інформаційної безпеки.
2. Життєво важливі інтереси особистості, суспільства та держави в інформаційній сфері.
3. Об'єкти та суб'єкти інформаційної безпеки.
4. Види інформаційної безпеки.
5. Концепція інформаційної безпеки держави.
6. Дестабілізуючі фактори інформаційної безпеки.
7. Визначення інформаційного середовища.
8. Класифікація загроз інформаційній безпеці.
9. Джерела загроз інформаційній безпеці.
10. Основні принципи забезпечення інформаційної безпеки.
11. Система забезпечення інформаційної безпеки держави.
12. Основні форми і способи забезпечення інформаційної безпеки держави.
13. Визначення поняття «інформаційне протиборство».
14. Інформаційна війна.
15. Концепція інформаційної війни.
16. Основні форми інформаційної війни
17. Військова теорія Клаузевіца
18. Сунь-цзи «Мистецтво війни»

19. Нікколо Мак'явеллі «Про військове мистецтво»
20. Міжнародні конфлікти та війни
21. Покоління війн
22. Типи воєн, що не вимагають фізичної присутності.
23. Статус інформації в сучасній інформаційній цивілізації.
24. Інструментарій комунікативних технологій: реклама, паблік рілейшнз, пропаганда довіри, інформаційна війна.
25. Моделі управління громадською думкою.
26. Творча і руйнівна сила інформації.
27. Публічна інформації і ухвалення політичних рішень.
28. Холодна війна СРСР-США як приклад інформаційної війни.
29. Приклади успішних інформаційних воєн в пострадянському світі.
30. Організація психологічних операцій у системі Північноатлантичного договору (НАТО).
31. Забезпечення психологічних операцій у США.
32. Інформаційні операції США в Афганістані (2001 р.) та Іраку (2003 р.).
33. Інформаційна операція країн НАТО проти Лівії 2011 року.
34. Інформаційна операція США та їхніх союзників проти Сирії 2013 року.
35. Інформаційне протиборство Росії та Грузії.
36. Інформаційна безпека України: мас-медійний аспект
37. Україна в умовах інформаційної війни – маніпулювання свідомістю
38. Український інтернет: мовний аспект
39. Інформаційна війна як складова частина ідеологічної боротьби.
40. Інформаційна війна між Україною й Росією.

Термінологічний словник

Бот-мережа – група автоматизованих акаунтів у соцмережах, які поширюють певні меседжі чи маніпулятивний контент.

Війна наративів – боротьба за інтерпретацію подій і формування потрібного світогляду.

Гібридна війна – форма війни, що поєднує військові, інформаційні, кібернетичні та економічні методи тиску.

Дезінформація – навмисне поширення неправдивих або перекручених даних для введення в оману цільової аудиторії.

Deepfake – штучно створене медіа (відео чи аудіо), що імітує реальних людей для маніпуляції свідомістю.

Ідеологічна диверсія – цілеспрямоване поширення ідей, що підривають національні інтереси.

Інформаційна асиметрія – нерівний доступ різних суб'єктів до інформації.

Інформаційна атака – цілеспрямоване використання інформаційних ресурсів для підриву авторитету, зниження довіри чи завдання шкоди об'єкту.

Інформаційна безпека – стан захищеності суспільства, держави та особи від деструктивного впливу у сфері інформації.

Інформаційна війна – сукупність дій держав, організацій чи акторів, спрямованих на здобуття переваги шляхом використання інформації як інструменту впливу, контролю чи знищення.

Інформаційний вплив – процес цілеспрямованої зміни свідомості чи поведінки суб'єкта через інформацію.

Інформаційні дії (акції) – це сукупність узгоджених за метою, завданнями, місцем і часом заходів, що проводяться силами і засобами, залученими для ведення інформаційної боротьби, протягом певного часу в певному районі (напрямку). Під час інформаційних дій можуть здійснюватися інформаційні удари.

Інформаційна диверсія – деструктивні інформаційні акції, спрямовані на підрив стабільності суспільства.

Інформаційна експансія – діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу з метою: поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії; витіснення положень національної ідеології і національної системи цінностей і заміщення їхніми власними цінностями й ідеологічними установками; збільшення ступеня свого

впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами.

Інформаційне забезпечення: підтримка засобами систем баз даних і баз знань процесів виробництва, торгівлі, керування, навчання, наукових досліджень та будь якої іншої діяльності в усіх сферах життя суспільства, які спрямовані на створення умов для задоволення інформаційних потреб людини, суспільства та держави.

Інформаційна зброя – технології, засоби та методи, що використовуються для ураження інформаційних систем, свідомості та поведінки людей.

Інформаційна зброя атаки – це інформаційна зброя, за допомогою якої здійснюється вплив на інформацію, що зберігається, обробляється й передається в інформаційно-обчислювальних мережах (ІОМ) і (або) порушуються інформаційні технології, що застосовуються в ІОМ.

Інформаційна зброя забезпечення – це інформаційна зброя, за допомогою якої здійснюється вплив на засоби захисту інформації об'єкта атаки, наприклад, інформаційно-обчислювальну систему. До складу інформаційної зброї забезпечення входять засоби комп'ютерної розвідки та засоби подолання системи захисту інформаційно-обчислювальної системи.

Інформаційні злочини можуть вчинятися із використанням як інформаційно комп'ютерних, так й інформаційно психологічних методів впливу.

Інформаційна інфраструктура: сукупність взаємодіючих систем виробництва, накопичення, збереження і розвитку інформаційних продуктів та їх доставки, виробництво інформаційних технологій, сервісного обслуговування інфраструктури й системи підготовки кадрів.

Інформаційна кооперація – форма забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними), що включає сукупність їхніх взаємоузгоджених дій, спрямованих на одержання відомостей про дестабілізуючі фактори, дестабілізуючі та інформаційні загрози й захист від них доступними законними способами й засобами.

Інформаційна операція (від лат. operatio – «дія») – це сукупність узгоджених за метою, завданнями, місцем і часом дій (акцій), ударів і битв, що проводяться за єдиним задумом і планом для вирішення завдань інформаційної боротьби (завоювання й утримання інформаційної переваги над противником або зниження його інформаційної переваги) на театрі воєнних дій, стратегічному або оперативному напрямках.

Інформаційний патронат (захисник) є формою забезпечення інформаційної безпеки фізичних і юридичних осіб із боку держави. Він припускає забезпечення органів управління системи інформаційної безпеки держави відомостями про дестабілізуючі фактори й загрози стану поінформованості фізичних і юридичних осіб (інформаційне забезпечення інформаційної безпеки) та власне захист життєво важливих інтересів цих осіб від інформаційних загроз, або, як ще кажуть, інформаційний захист.

Інформаційна перевага розуміють ситуацію, що надає можливість змінити уявлення противника про дійсну обстановку й позбавити його здатності прогнозувати подальші події та впливати на них.

Інформаційне протиборство, яке характеризується, з однієї сторони, впливом на системи добування, оброблення, розповсюдження та зберігання інформації противника, а з іншої — застосуванням заходів захисту своїх подібних систем від деструктивного та керуючого впливу.

Інформаційна операція – скоординований комплекс дій для досягнення інформаційної переваги.

Інформаційний простір – середовище циркуляції інформації, що охоплює канали комунікації, технічні системи та суспільну свідомість.

Інформаційний суверенітет – здатність держави контролювати й регулювати потоки інформації поза межами держави з метою дотримання законів України, прав і свобод громадян, забезпечення національної безпеки держави.

Під **інформаційним ударом** розуміють короточасний потужний узгоджений інформаційний вплив сил і засобів на найбільш важливий елемент (елементи) системи управління (керування) противника для досягнення

рішучих цілей із завоювання інформаційної переваги (зниження інформаційної переваги противника).

Кіберзагрози – атаки або дії, що ставлять під небезпеку інформаційні системи, мережі та дані.

Кіберзброя – програмні або апаратні засоби, що застосовуються для проведення кібератак.

Кібервійна – бойові дії у кіберпросторі з метою ураження інформаційних систем противника.

Кібертероризм – використання кіберпростору для здійснення терористичних актів.

Когнітивна війна – форма інформаційного протистояння, спрямована безпосередньо на свідомість та мислення людини.

Контрпропаганда – заходи протидії чужій пропаганді.

Контроль над свідомістю (mind control) – методи впливу на психіку з метою управління поведінкою.

Маніпуляція – прихований вплив на свідомість людини чи групи з метою зміни їх поведінки в потрібному напрямку.

Мета інформаційної боротьби – забезпечення необхідного ступеня власної інформаційної безпеки й максимальне зменшення рівня інформаційної безпеки конфронтуючої сторони. Досягнення мети інформаційної боротьби здійснюється шляхом вирішення багатьох завдань, основними з яких є ураження об'єктів інформаційної сфери конфронтуючої сторони і захист власної інформації.

Метод оцінки ефективності інформаційної боротьби – це сукупність способів, прийомів визначення кількісних значень показників інформованості протидіючих сторін та розрахунку ступеня інформаційної переваги однієї з них над іншою відповідно до мети інформаційної боротьби. В основу методу може бути покладене математичне моделювання процесу забезпечення інформацією органів управління протидіючих сторін.

Міждержавні дестабілізуючі фактори – це конфлікти різноманітних масштабів і проявів (в економіці, політиці, ідеології, дипломатії тощо).

Напрями забезпечення безпеки інформації – це нормативно-правові категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, на рівні підприємства або організації, на рівні окремої особи.

Наступальна інформаційна операція має за мету завоювання інформаційної переваги над противником. У цій операції головні зусилля спрямовуються на дезорганізацію його систем управління військами і зброєю, а частина сил та засобів забезпечують стійкість власного управління. При цьому всі заходи, які проводяться в межах інформаційної боротьби, повинні забезпечувати сприятливі умови для бойових дій своїх військ (сил).

Наступальні способи інформаційної боротьби реалізують блокування інформації, відвернення уваги, сковування сил противника, вимотування противника, інсценування, дезінтеграцію, замирення, залякування противника, провокування противника, перевантаження противника, навіювання на противника і тиск на противника.

Національна безпека – категорія політичної науки (політології), що характеризує стан соціальних інститутів, що забезпечує їхню ефективну діяльність для підтримки оптимальних умов існування особистості, суспільства та держави. Вона відображає зв'язок безпеки з нацією.

Медійна війна – використання ЗМІ для поширення вигідних повідомлень і дискредитації супротивника.

Медіаграмотність – здатність критично оцінювати інформацію та протидіяти маніпуляціям.

Оборонна інформаційна операція проводиться в умовах великої інформаційної переваги противника і має за мету зниження цієї переваги. У такій операції головні зусилля сил і засобів спрямовуються на забезпечення інформаційної безпеки органів управління об'єднань і з'єднань, на захист інформації в системах керування. Частина сил і засобів спрямовуються на дезорганізацію управління військами і зброєю противника.

Оборонні способи інформаційної боротьби реалізують деблокування та ототожнення інформації.

Оперативна безпека – це комплекс заходів із виявлення критичної інформації, проведення аналізу дій своїх збройних сил.

Особистість – людина як суб'єкт відносин і свідомої діяльності. До життєво важливих інтересів особистості належать, насамперед права і свободи людини й громадянина, зокрема інформаційні.

Оцінка ефективності інформаційної боротьби – це визначення ступеня відповідності результатів інформаційної боротьби її меті (цілі).

Пасивне забезпечення інформаційної безпеки передбачає реагування на вже наявні загрози, спрямоване на безпосередню протидію акціям, що є деструктивними щодо соціальної системи.

Поінформованість особистості (суспільства та держави) – задоволення в будь якій мірі потреб в інформації, що призводить до оволодіння відомостями про навколишній світ та процеси, що відбуваються у ньому.

Правильне інформування – це передавання органу керування неспотвореної інформації про істинну ситуацію.

Правильне дезінформування – це передавання органу керування неспотвореної інформації про неправдиву ситуацію.

Правовий захист інформації як ресурсу признаний на міждержавному, державному рівні та визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом та ліцензіями на їхній захист. На державному рівні правовий захист регулюється державними та відомчими актами.

Принципи інформаційної боротьби – це науково обґрунтовані положення, правила, рекомендації з підготовки і ведення інформаційної боротьби, керівництва її силами й засобами. Вони створюються на основі законів і закономірностей, а також досвіду, набутого в результаті практичної діяльності в галузі інформаційної боротьби. Принципи інформаційної боротьби не тільки відображають об'єктивну сутність, але і приписують, як слід діяти в конкретних умовах. Зміст і масштаби завдань інформаційної боротьби передбачають наявність цілої множини принципів інформаційної боротьби.

Пропаганда – систематичне поширення ідей, доктрин чи поглядів для формування громадської думки на користь певних політичних, військових або ідеологічних цілей.

Пропагандистський наратив – стійка схема подання інформації, яка формує потрібну картину світу.

Пропагандистська машина – система інституцій та засобів, які забезпечують масове поширення пропаганди.

Психологічні операції (PSYOPS) – комплекс заходів, спрямованих на вплив на свідомість та поведінку противника чи населення з метою досягнення політичних і військових цілей.

Силові способи інформаційної боротьби засновані на ураженні об'єктів інформаційної боротьби різноманітними видами зброї (звичайної, радіоелектронної, інформаційної). Застосування силових способів дозволяє досягти інформаційної переваги в кількості інформації, необхідної для вирішення завдань управління військами (силами).

Система забезпечення національної безпеки – організована державою сукупність суб'єктів: державних органів, громадських організацій, посадових осіб та окремих громадян, об'єднаних цілями та завданнями щодо захисту національних інтересів, що здійснюють узгоджену діяльність у межах законодавства держави.

Система захисту державної таємниці – сукупність органів захисту державної таємниці, використовуваних ними засобів і методів захисту відомостей, що становлять державну таємницю та їх носіїв, а також заходів, що проводяться з цією метою.

Спосіб блокування інформації полягає в тому, що на етапі підготовки й у ході бойових дій шляхом виконання комплексу заходів інформаційної протидії повністю або частково припиняється добування (збирання) інформації про ситуацію й обмін інформацією в системах управління військами і зброєю противника. Для реалізації цього способу застосовується вогневе, радіоелектронне й інформаційне ураження (придушення) елементів систем управління військами (силами) і зброєю противника.

Спосіб відвернення уваги полягає в тому, що на етапі підготовки бойових дій шляхом проведення комплексу заходів інформаційної протидії намагаються створити реальну або удавану загрозу для одного з найбільш уразливих місць противника і тим самим переконати його у своїх намірах діяти на одному з можливих напрямів з метою відволікти головні сили противника на вирішення другорядних завдань.

Спосіб вимотування противника полягає в проведенні комплексу заходів інформаційної протидії з метою примусити противника здійснювати не вигідні й марні дії і, як наслідок, вступити в бій із розтраченими ресурсами та зниженою боєздатністю. При цьому можуть проводитися обмежені бойові або відволікаючі дії.

Спосіб деблокування інформації передбачає проведення комплексу заходів інформаційного захисту з метою одержання інформації, яка приховується або модифікується противником. При цьому можуть застосовуватися всі можливі методи, сили і засоби, аж до проведення широкомасштабних операцій.

Спосіб дезінтеграції використовується для вирішення політичних завдань у міждержавних конфліктах. Реалізація способу полягає в проведенні комплексу заходів інформаційної протидії, що дозволяє нав'язати противникові уяву про необхідність діяти всупереч коаліційним інтересам. З цією метою може використовуватися дезінформування громадської думки, а також формування фальшивих уявлень про воєнно-політичну ситуацію у голів держав, що беруть участь у конфлікті. Крім того, можуть проводитися заходи, які сприяють загостренню реально наявних або штучно створюваних суперечностей у стані ворога з метою зменшити його воєнну й економічну могутність.

Спосіб замирення застосовується для нав'язування противникові уяви про нейтральну або союзницьку позицію конфронтуючої сторони. Суть способу полягає у проведенні комплексу заходів інформаційної протидії, основною метою яких є створення у противника уяви про те, що здійснюється не підготовка до бойових дій, а планова оперативна (бойова підготовка) або будь-які інші заходи. Противник повинен упевнитися в дружніх або мирних намірах

конфронтуючої сторони і втратити пильність. Таємно ж планується і готується напад на нього при першому зручному випадку.

Спосіб інсценування полягає в тому, що на етапі підготовки до бойових дій противникові нав'язується уява про наявність удаваної загрози для одного з його уразливих місць, запобігання якій не потребує виділення сил та засобів. Це робиться з метою, щоб противник помітив обман і його пильність була б приспана. Якщо виникає справжня загроза, він також сприйме її як фальшиву і зможе діяти відповідно до реальної ситуації.

Спосіб навіювання на противника полягає у формуванні й наступному використанні інформаційного стереотипу конфронтуючої сторони. Для цього на етапі підготовки й у ході бойових дій шляхом проведення комплексу заходів інформаційної протидії до відома противника доводиться інформація, яка має юридичну, моральну, ідеологічну або іншу силу і спонукає його до здійснення будь-яких дій, вигідних конфронтуючій стороні.

Спосіб ототожнення інформації передбачає проведення комплексу заходів інформаційного захисту, які забезпечують збирання і зіставлення інформації про один і той же факт (явище) від різноманітних джерел, що дозволяє виявити і блокувати дезінформацію, яка розповсюджується противником.

Спосіб провокування противника призначений для спонукання противника до здійснення будь-яких дій, корисних протилежній стороні. Спосіб перевантаження противника полягає в тому, щоб на етапі підготовки й у ході бойових дій довести до противника таку кількість суперечливої інформації, яка перевантажує його систему управління, і змушує приймати й реалізовувати рішення в умовах підвищеної невизначеності ситуації.

Спосіб сковування сил противника є різновидом способу відвернення уваги. При його застосуванні у противника створюється переконання в наявності загрози для одного з уразливих місць, запобігання якій потребує виділення частини сил.

Спосіб тиску на противника заснований на доведенні до суспільної думки відомостей, які ганьблять противника, та змушують державні, міждержавні,

суспільні та інші організації здійснювати дії, які ускладнюють виконання його задумів.

Спін-докторинг – спеціальні технології створення позитивного іміджу або пом'якшення негативної інформації.

Сублімінаційний вплив – передача інформації на підсвідомому рівні.

Стратегічні комунікації – узгоджена діяльність держави чи організації, спрямована на донесення повідомлень і формування позитивного іміджу.

Тролінг – провокаційні дії в онлайн-середовищі з метою конфлікту, дискредитації чи відволікання уваги.

Фейк – вигадана або сфабрикована інформація, подана як достовірна.

Фейк-ньюз (Fake News) – неправдиві новини, створені для маніпуляції суспільною думкою.

Хакерська атака – несанкціоноване втручання у роботу інформаційної системи.

Хактивізм – використання хакерських методів для політичних чи соціальних цілей.

Цензура – контроль за поширенням інформації державними чи іншими органами.

Цільова аудиторія – група людей, на яку спрямовані інформаційні впливи чи кампанії.

Рекомендована література

1. Гамова І. В. Інформаційні війни : підручник / І. В. Гамова. Київ : Держ. торг.-екон. ун-т, 2022. 184 с.
2. Гібридна війна і журналістика. Проблеми інформаційної безпеки: навчальний посібник / за заг. ред. В. О. Жадька. Київ: Вид-во НПУ імені М. П. Драгоманова, 2018. 356 с.
3. Горбулін В. Світова гібридна війна: український фронт: монографія / за заг. ред. В.П. Горбуліна. Київ: НІСД, 2017. 496 с.
4. Інформаційна війна і національна безпека: монографія / П. П. Ткачук [та ін.]. Львів: Акад. сухопут. військ, 2015. 264 с.

5. Інформаційні війни: монографія / Д. В. Кіслов. Київ. Нац. торг.-екон. ун-т. Київ. 2013. 300 с.
6. Інформаційні війни у соціальних он-лайн-мережах: [монографія] / Курбан О. В. ; Київ. ун-т ім. Бориса Грінченка. Київ: Київ. ун-т ім. Бориса Грінченка, 2017. 392 с.
7. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської. Київ: НІСД, 2016. 109 с
8. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах / П. С. Прибутко, І. Б. Лук'янець. Київ: Поливода А. В., 2007. 252 с.
9. Історія інформаційно-психологічного протиборства: підруч. / за заг. ред. д.ю.н., проф., засл. юриста України Є.Д.Скулиша. Київ: Наук.-вид. відділ НА СБ України, 2012. 212 с.
10. Магда Є.В. Гібридна віна – вижити і перемогти. Харків: Віват, 2015. 604 с.
11. Почепцов Г. Сучасні інформаційні війни. Вид. 2-ге, допов. Київ: КиєвоМогил. акад., 2016. 502 с.
12. Сенси і війни: Україна і Росія в інформаційній і смисловій війнах. Георгій Почепцов; пер. з рос. Тамари Гуменюк. Київ: Києво-Могил. акад., 2016. 312 с.
13. Худолій А. О. Інформаційна війна 2014-2022 рр. : монографія. Острого : Видавництво Національного університету «Острозька академія», 2022. 208 с.

Додаткова

1. Біла книга протидії дезінформації. Київ: ГО «Інститут інформаційної безпеки» 2022. 62 с.
2. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. Київ: ДУТ. 2015. 288 с.
3. Зелена книга протидії дезінформації / Упоряд. і заг. ред. С. Балан. Київ: ГО «Інститут інформаційної безпеки». 2022. 178 с.

4. Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін Рада нац. безпеки і оборони України; Ін-т проблем нац. безпеки. Київ: Інтертехнологія, 2009. 164 с.
5. Інформаційно-психологічне протиборство (еволюція та сучасність): монографія / Я. М. Жарков [та ін.]; Військ. ін-т Київ. нац. ун-ту ім. Т. Г. Шевченка. Київ: Віпол, 2013. 247 с.
6. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі : навчальний посібник / О.В.Курбан. Київ: ВІКНУ, 2016. 286 с.
7. Національна безпека в умовах інформаційних та гібридних війн: монографія за заг. ред. В. Куйбіди і В. Бебика; Нац. акад. держ. упр. при Президентові України, Ред. пол.-укр. журн. «Соц.-гуманітар. Науки». Київ: НАДУ, 2019. 380 с.

Інформаційні ресурси

1. Національна бібліотека України імені В. І. Вернадського, електронні фахові видання // www.nbuv.gov.ua
2. Львівська національна наукова бібліотека імені В. Стефаника // <http://www.library.lviv.ua/>
3. Національна історична бібліотека України // <http://www.dibu.kiev.ua/>
4. Національна парламентська бібліотека України // <http://www.nplu.org/>
5. Харківська державна наукова бібліотека України імені В. Короленка // <http://korolenko.kharkov.com/>
6. Наукова бібліотека ім.В. Максимовича Київського національного університету імені Тараса Шевченка // <http://lib-gw.univ.kiev.ua/>
7. Наукова бібліотека Львівського національного університету імені Івана Франка // <http://library.lnu.edu.ua/bibl/>
8. Офіційний сайт Ради національної безпеки і оборони України <http://www.rainbow.gov.ua/>
9. Національний інститут стратегічних досліджень <http://www.niss.gov.ua/>