

Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Кафедра міжнародних відносин, міжнародної інформації та безпеки

“ЗАТВЕРДЖУЮ”

Проректор з науково-педагогічної
роботи

Антон ПАНТЕЛЕЙМОНОВ



08 2021 р.

Робоча програма навчальної дисципліни

Інформаційна безпека та інформаційні війни

(назва навчальної дисципліни)

рівень вищої освіти перший (бакалаврський)

галузь знань 29 «Міжнародні відносини»

спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»

освітня програма «Міжнародні відносини»

вид дисципліни за вибором

факультет міжнародних економічних відносин та туристичного бізнесу

2021 / 2022 навчальний рік

Програму рекомендовано до затвердження Вченою радою факультету міжнародних економічних відносин та туристичного бізнесу

«27» серпня 2021 року, протокол № 1

РОЗРОБНИК ПРОГРАМИ: доктор історичних наук, професор, професор кафедри міжнародних відносин, міжнародної інформації та безпеки Олександр КАПЛІН.

Програму схвалено на засіданні кафедри міжнародних відносин, міжнародної інформації та безпеки

Протокол від «26» серпня 2021 року № 1

Завідувачка кафедри


(підпис)

Людмила НОВІКОВА
(ім'я та прізвище)

Програму погоджено з гарантом освітньо-професійної програми «Міжнародні відносини»

Гарант освітньо-професійної програми
«Міжнародні відносини»


(підпис)

Євгенія СОЛОВИХ
(ім'я та прізвище)

Програму погоджено науково-методичною комісією факультету міжнародних економічних відносин і туристичного бізнесу

Протокол від «26» серпня 2021 року № 1

Голова науково-методичної комісії


(підпис)

Лариса ГРИГОРОВА – БЕРЕНДА
(ім'я та прізвище)

ВСТУП

Програма навчальної дисципліни «Інформаційна безпека та інформаційні війни» складена відповідно до освітньо-професійної програми «Міжнародні відносини» підготовки бакалаврів за спеціальністю 291 «Міжнародні відносини».

Даний курс присвячений аналізу теоретико-методологічних і практичних аспектів інформаційних воєн, розгляду інформаційно-технічних та інформаційно-психологічних сторін інформаційного впливу в сучасному світі, вивченню фактичних матеріалів з основних розділів курсу.

1. Мета та завдання навчальної дисципліни

1.1. Мета викладання навчальної дисципліни: дати здобувачам цілісне уявлення про інформаційну безпеку, інформаційні війни, їх історію, особливості прояву на початку XXI століття, загрози в інформаційній сфері та завдання щодо забезпечення інформаційної безпеки.

1.2. Основними завданнями вивчення навчальної дисципліни є:

- формування наступних загальних компетентностей:

- здатність до абстрактного мислення, аналізу та синтезу;
- знання та розуміння предметної області спеціальності «Міжнародні відносини, суспільні комунікації та регіональні студії» та розуміння професійної діяльності;
- здатність вчитися і оволодівати сучасними знаннями та застосовувати їх у практичній діяльності;
- здатність спілкуватися державною та іноземними мовами як усно, так і письмово;
- здатність до пошуку, оброблення та аналізу інформації з різних джерел, зокрема завдяки використанню інформаційних і комунікаційних технологій;
- вміння виявляти, ставити та вирішувати проблеми;

- формування наступних фахових компетентностей:

- поглиблені знання про природу, динаміку, принципи організації міжнародних відносин, типи та види міжнародних акторів, сучасні тенденції розвитку світової політики;
- розуміння сутності процесів глобалізації та їх впливу на міжнародні відносини;
- здатність аналізувати та прогнозувати міжнародні відносини у різних контекстах, зокрема політичному, безпековому, правовому, економічному, суспільному, культурному та інформаційному;
- поглиблені знання про теоретичні та прикладні дослідження міжнародних відносин і світової політики у політичній, економічній, юридичній науках, у міждисциплінарних дослідженнях;
- поглиблені знання про природу та джерела зовнішньої політики, еволюцію підходів до формування та здійснення зовнішньої політики, принципи організації системи зовнішньої політики та функціонування інститутів зовнішньої політики;
- здатність провадити прикладні аналітичні розробки проблем міжнародних відносин та світової політики, фахово готувати аналітичні матеріали та довідки;
- розуміння особливостей розвитку країн та регіонів, сучасних глобальних, регіональних та локальних процесів, та місця в них України;
- здатність виробляти підходи до розв'язання проблем і завдань у сфері міжнародних відносин, міжнародної та національної безпеки, зовнішньої політики (зокрема, міжнародних та внутрішньодержавних конфліктів).

1.3. Кількість кредитів – 3

1.4. Загальна кількість годин - 90

1.5. Характеристика навчальної дисципліни

За вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
4-й	
Семестр	

8-й	
Лекції	
36 год.	
Семінарські заняття	
12 год.	
Самостійна робота	
42 год.	
Індивідуальні завдання	
-	

1.6. Заплановані результати навчання

Згідно з вимогами освітньо-професійної програми студенти повинні досягти таких результатів навчання:

Знання:

- Фундаментальні знання щодо природи, джерел та напрямів еволюції міжнародних відносин, міжнародної політики, зовнішньої політики держав, стану теоретичних досліджень міжнародних відносин та світової політики;
- Поглиблені знання проблем міжнародної та національної безпеки, міжнародних та інтернаціональних конфліктів, підходів, способів та механізмів забезпечення безпеки у міжнародному просторі та зовнішній політиці держав;

Уміння:

- Демонструвати системне сприйняття та розуміння положень, які відносяться до галузі знань «Міжнародні відносини» або є складовою професійної практики;
- Визначати та прогнозувати політичні, дипломатичні, безпекові, суспільні і інші ризики у сфері міжнародних відносин та глобального розвитку
- Оцінювати та аналізувати міжнародні зовнішньополітичні проблеми та ситуації, пропонувати підходи до вирішення таких проблем.

2. Тематичний план навчальної дисципліни

Розділ 1. Теоретико-методологічні проблеми вивчення інформаційної безпеки та інформаційних воєн.

Тема 1. Інформаційне суспільство, інформаційна безпека та інформаційні війни.

Гене́за наукових досліджень інформаційного суспільства та інформаційної безпеки. Інформаційна безпека як складова національної безпеки. Інформаційна безпека та безпека інформації. Загрози в інформаційній сфері.

Поняття та сутність інформаційної безпеки країни. Механізм забезпечення національної інформаційної безпеки. Державна політика України в сфері національного інформаційного простору. Національні інтереси в інформаційній сфері. Політика формування національного інформаційного простору. Інформаційна безпека у сучасному світі. Стратегія інформаційної безпеки. Власники інформації, що захищається. Класифікація інформації за ступенем її таємності. Безпека інформації в комерційних мережах. Міжнародний аспект захисту інформації.

Зародження концепції інформаційного суспільства. Інформаційне суспільство як середовище організації та проведення інформаційних воєн.

Створення глобального інформаційного простору. Розвиток інформаційного суспільства в західних країнах.

Інформаційне суспільство та інформаційні війни.

Тема 2. Сутність інформаційних воєн, принципи ведення та засоби забезпечення.

Основні поняття: «інформаційна війна», «інформаційне протистояння», «інформаційний вплив», «ідеологічна боротьба», «психологічна війна», «пропаганда», «кібервійна», «мережева війна», «гібридна війна». Характеристики інформаційної війни. Об'єкти інформаційної війни: інформаційні системи, інформаційні процеси, масова свідомість, громадська думка, індивідуальна свідомість. Наступальні і оборонні інформаційні війни. Види інформаційної зброї і способи його застосування. Особливості застосування інформаційної зброї.

Засоби впливу в інформаційних війнах: психотронна зброя, Інтернет, хакери, блогери, відеоігри, інформаційний тероризм у всесвітній глобальній мережі, засоби масової інформації.

Тема 3. Дослідження з проблем інформаційних і інформаційно-психологічних воєн: етапи, напрямки, підходи.

Основні етапи досліджень інформаційних і інформаційно-психологічних воєн. Характер сучасних досліджень про інформаційні та інформаційно-психологічні війни.

Дослідження проблем інформаційної безпеки. Розробка концепції державної інформаційної політики в умовах інформаційного суспільства та інформаційної війни.

Тема 4. Історичні етапи формування теорії і практики інформаційних воєн.

Розвиток форм і способів психологічного впливу на противника. Проблеми інформаційного протиборства в Новий час. Розвиток засобів масової інформації в XIX столітті і інформаційне протиборство в період збройних конфліктів і воєн.

Інформаційне протиборство в роки Першої світової війни. Розвиток засобів масової інформації та їх роль в пропагандистських операціях. Розробка принципів ведення пропагандистських кампаній.

Інформаційне протиборство в роки Другої світової війни. Організація тотальної пропаганди в нацистській Німеччині. Діяльність органів пропаганди Великобританії і США. Напрями діяльності органів спецпропаганди СРСР.

Розділ 2. Інформаційне протиборство др. пол. XX ст.- поч. XX ст.

Тема 5. Інформаційне протиборство у др. пол.–напр. XX століття.

Трансформація інформаційних воєн в новітній час. Інформаційно-ідеологічне протистояння між СРСР і США. Промова У. Черчілля у Фултоні, як початок холодної війни. Психологічна війна і ідеологічна боротьба.

Органи психологічної війни США, Великобританії, ФРН та напрямки їх діяльності в інформаційному протиборстві з СРСР.

Політика СРСР на прискорення, гласність і демократизацію. Концепція нового політичного мислення інформаційне протиборство.

Тема 6. Інформаційне протиборство на початку XXI століття.

Особливості інформаційних воєн на початку XXI століття. Використання інформаційних технологій. Учасники, методи, засоби, прийоми.

Боротьба проти терористичної організації «Ісламська держава» і інформаційне протиборство.

Тема 7. Інформаційно-психологічна війна як засіб агресії і досягнення політичних цілей.

Поняття інформаційно-психологічної війни. Місце психологічної війни в системі інформаційної війни. Основні структурні елементи інформаційно-психологічного впливу. Дезінформування, лобіювання, маніпулювання, пропаганда, управління кризами, шантаж. Основні етапи заходів і аксіоми психологічної війни.

Інформаційно-психологічні операції: зміст, класифікація, цілі і об'єкти. Методи психологічних операцій в інформаційних війнах. Органи психологічної війни західних держав. Цілі та об'єкти психологічних операцій.

Роль засобів масової інформації в інформаційно-психологічних війнах.

Тема 8. Кібервійна як вид інформаційних воєн. Мережеві війни і їх особливості.

Кібервійна як інформаційне протиборство в кіберпросторі.

Зарубіжні і вітчизняні вчені про кібервійну. Цілі кібервійни: дестабілізація комп'ютерних систем, порушення доступу до Інтернету державних установ і ділових центрів, створення безладу і хаосу в житті країн. форми прояву кібервійни: вандалізм, пропаганда, шпигунство, атаки на комп'ютерні системи і сервери.

Напрямок діяльності різних держав з протидії кібератак.

Мережеві війни і їх особливості. Поняття мережевого суспільства і мережі.

Особливості мережевого суспільства.

Концепції сетецентричної війни. Принципи ведення мережевих воєн. Участь приватних військових компаній і неурядових організацій в мережевих війнах.

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усь ого	у тому числі					усь ого	у тому числі				
		л	с	лаб	інд	с.р.		л	с	лаб	інд	с.р.
Розділ 1. Теоретико-методологічні проблеми вивчення інформаційної безпеки та інформаційних воєн.												
Тема 1. Інформаційне суспільство, інформаційна безпека та інформаційні війни.	18	8	2			8						
Тема 2. Сутність інформаційних воєн, принципи ведення та засоби забезпечення.	9	4	1			4						
Тема 3. Дослідження з проблем інформаційних і інформаційно-психологічних воєн: етапи, напрями, підходи.	9	4	1			4						
Тема 4. Історичні етапи формування теорії і практики інформаційних воєн.	12	4	2			6						
Разом за розділом 1	48	20	6			22						
Розділ 2. Інформаційне протиборство др. пол. XX ст.- поч. XXI ст.												
Тема 5. Інформаційне протиборство у др. пол.– напр. XX століття.	10	4	1			5						
Тема 6. Інформаційне протиборство на початку XXI століття.	11	4	2			5						
Тема 7. Інформаційно-психологічна війна як засіб агресії і досягнення політичних цілей.	10	4	1			5						
Тема 8. Кібервійна як вид інформаційних воєн. Мережеві війни і їх особливості.	11	4	2			5						
Разом за розділом 2	42	16	6			20						
Усього годин	90	36	12			42						

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
	Тема 1. Інформаційне суспільство, інформаційна безпека та інформаційні війни. Гене́за наукових досліджень інформаційного суспільства та інформаційної безпеки. Інформаційна безпека як складова національної безпеки.	2

	Інформаційна безпека та безпека інформації. Загрози в інформаційній сфері. Поняття та сутність інформаційної безпеки країни. Механізм забезпечення національної інформаційної безпеки. Державна політика України в сфері національного інформаційного простору. Національні інтереси в інформаційній сфері. Політика формування національного інформаційного простору. Інформаційна безпека у сучасному світі. Стратегія інформаційної безпеки. Власники інформації, що захищається. Класифікація інформації за ступенем її таємності. Безпека інформації в комерційних мережах. Міжнародний аспект захисту інформації. Зародження концепції інформаційного суспільства. Інформаційне суспільство як середовище організації та проведення інформаційних воєн. Створення глобального інформаційного простору. Розвиток інформаційного суспільства в західних країнах. Інформаційне суспільство та інформаційні війни.	
	Тема 2. Сутність інформаційних воєн, принципи ведення та засоби забезпечення. Основні поняття: «інформаційна війна», «інформаційне протиборство», «інформаційний вплив», «ідеологічна боротьба», «психологічна війна», «пропаганда», «кібервійна», «мережева війна», «гібридна війна». Характеристики інформаційної війни. Об'єкти інформаційної війни. Види інформаційної зброї і способи його застосування. Особливості застосування інформаційної зброї. Засоби впливу в інформаційних війнах.	1
	Тема 3. Дослідження з проблем інформаційних і інформаційно-психологічних воєн: етапи, напрямки, підходи. Основні етапи досліджень інформаційних і інформаційно-психологічних воєн. Характер сучасних досліджень про інформаційні та інформаційно-психологічних війнах. Дослідження проблем інформаційної безпеки. Розробка концепції державної інформаційної політики в умовах інформаційного суспільства та інформаційної війни.	1
	Тема 4. Історичні етапи формування теорії і практики інформаційних воєн. Розвиток форм і способів психологічного впливу на противника. Проблеми інформаційного протиборства в Новий час. Розвиток засобів масової інформації в XIX столітті і інформаційне протиборство в період збройних конфліктів і воєн. Інформаційне протиборство в роки Першої світової війни. Розвиток засобів масової інформації та їх роль в пропагандистських операціях. Розробка принципів ведення пропагандистських кампаній. Інформаційне протиборство в роки Другої світової війни. Організація тотальної пропаганди в нацистській Німеччині. Діяльність органів пропаганди Великобританії і США. Напрями діяльності органів спецпропаганди СРСР.	2
	Тема 5. Інформаційне протиборство у др. пол.–напр. XX століття. Трансформація інформаційних воєн в новітній час. Інформаційно-ідеологічне протистояння між СРСР і США.	1

	Промова У. Черчілля у Фултоні, як початок холодної війни. Психологічна війна і ідеологічна боротьба. Органи психологічної війни США, Великобританії, ФРН та напрямки їх діяльності в інформаційному протиборстві з СРСР. Політика СРСР на прискорення, гласність і демократизацію. Концепція нового політичного мислення інформаційне протиборство.	
	Тема 6. Інформаційне протиборство на початку XXI століття. Особливості інформаційних воєн на початку XXI століття. Використання інформаційних технологій. Учасники, методи, засоби, прийоми.	2
	Тема 7. Інформаційно-психологічна війна як засіб агресії і досягнення політичних цілей. Поняття інформаційно-психологічної війни. Місце психологічної війни в системі інформаційної війни. Основні структурні елементи інформаційно-психологічного впливу. Основні етапи заходів і аксіони психологічної війни. Інформаційно-психологічні операції: зміст, класифікація, цілі і об'єкти. Методи психологічних операцій в інформаційних війнах. Органи психологічної війни західних держав. Цілі та об'єкти психологічних операцій. Роль засобів масової інформації в інформаційно-психологічних війнах.	1
	Тема 8. Кібервійна як вид інформаційних воєн. Мережеві війни і їх особливості. Кібервійна як інформаційне протиборство в кіберпросторі. Цілі кібервійни. Форми прояву кібервійни. Напрямок діяльності різних держав з протидії кібератак. Мережеві їх особливості. Концепції сетецентричної війни.	2
	Разом	12

5. Завдання для самостійної роботи

№ з/п	Види, зміст самостійної роботи	Кількість годин	Форма контролю
1.	Тема 1. Інформаційне суспільство, інформаційна безпека та інформаційні війни. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, підготувати завдання за темою.	8	усне опитування
2.	Тема 2. Сутність інформаційних воєн, принципи ведення та засоби забезпечення. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття,	4	усне опитування

	відповісти на запитання для контролю знань, підготувати завдання за темою.		
3.	Тема 3. Дослідження з проблем інформаційних і інформаційно-психологічних воєн: етапи, напрямки, підходи. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, підготувати завдання за темою.	4	усне опитування
4.	Тема 4. Історичні етапи формування теорії і практики інформаційних воєн. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, підготувати завдання за темою.	6	усне опитування
5.	Тема 5. Інформаційне протиборство у др. пол.–напр. XX століття. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, підготувати завдання за темою.	5	усне опитування
6.	Тема 6. Інформаційне протиборство на початку XXI століття. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, підготувати завдання за темою.	5	усне опитування
7.	Тема 7. Інформаційно-психологічна війна як засіб агресії і досягнення політичних цілей. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, підготувати завдання за темою.	5	усне опитування
8.	Тема 8. Кібервійна як вид інформаційних воєн. Мережеві війни і їх особливості. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, підготувати завдання за темою.	5	усне опитування

	Разом	42	
--	-------	----	--

6. Індивідуальні завдання

Навчальним планом не передбачено.

7. Методи навчання.

Відповідність методів навчання та форм оцінювання визначеним результатам навчання за ОПП віддзеркалює табл. 7.1

Таблиця 7.1

Методи навчання та засоби діагностики результатів навчання за освітньою компонентною «Інформаційна безпека та інформаційні війни»

Шифр ПРН (відповідно до ОНП)	Результати навчання (відповідно до ОПП)	Методи навчання	Засоби діагностики /форми оцінювання
РН09	<i>Здійснювати опис та аналіз міжнародної ситуації, збирати з різних джерел необхідну для цього інформацію про міжнародні та зовнішньополітичні події та процеси.</i>	Лекція; пошук джерел інформації (критичний аналіз, інтерпретація), корегування та підготовка частини наукового дослідження, її презентація	Оцінювання усних відповідей на практичних заняттях, оцінювання аналітичної частини дослідження, залікова робота
РН12	<i>Вільно спілкуватися державною та іноземними мовами на професійному рівні, необхідному для ведення професійної дискусії, підготовки аналітичних та дослідницьких документів.</i>	Лекція, надання зворотного зв'язку, аналіз отриманих результатів	Оцінювання результатів дослідження на практичних заняттях; тестових завдань, розв'язування аналітичних задач, оцінювання роботи над науковим текстом, залікова робота
РН13	<i>Здійснювати прикладний аналіз міжнародних відносин, зовнішньої політики України та інших держав, міжнародних процесів та міжнародної ситуації відповідно до поставлених цілей, готувати інформаційні та аналітичні матеріали.</i>	Лекція, надання зворотного зв'язку, аналіз отриманих результатів, презентація результатів досліджень	Оцінювання виконання творчих завдань, аналітичних, залікова робота

Замість виконання завдань (вивчення тем) можуть також додатково враховуватись такі види активностей здобувача:

– участь у науково-дослідних та прикладних дослідженнях з проблем використання сучасних освітніх технологій (презентації результатів).

Під час вивчення дисципліни «Інформаційна безпека та інформаційні війни» застосовуються наступні 3 групи методів навчання:

1. Методи організації і здійснення навчально-пізнавальної діяльності – це вербальні методи і сприймання навчальної інформації (розповідь, лекція), наочні (ілюстрація, презентація), практичні (виконання групових та індивідуальних завдань)

2. Методи стимулювання і мотивації навчально-пізнавальної діяльності – застосування дискусій
3. Методи контролю і самоконтролю за ефективністю навчально-пізнавальної діяльності. В межах самостійної роботи передбачається робота з джерелами і літературою, робота з методичними матеріалами, робота з інтернет-джерелами, виконання творчих завдань. При вивченні курсу активно використовуються інтерактивні методи (при проведенні лекцій та практичних занять) та проблемно-пошукові методи навчання (як при проведенні аудиторних занять, так і при організації самостійної роботи здобувачів).

8. Методи контролю

При вивченні дисципліни застосовується поточний та підсумковий семестровий форми контролю. Також, передбачено обов'язковий контроль засвоєння навчального матеріалу дисципліни, віднесеного на самостійну роботу.

Поточний контроль (засвоєння окремих тем) проводиться у формі усного опитування або письмового експрес-контролю на лекціях та семінарських заняттях, у формі виступів здобувачів з доповідями при обговоренні навчальних питань на семінарських заняттях.

Підсумковий семестровий контроль з дисципліни є обов'язковою формою контролю навчальних досягнень студента.

Підсумковий семестровий контроль здійснюється під час проведення заліку. Загальна кількість балів за успішне виконання залікових завдань – 40. Час виконання – до 80 хвилин

Вміст залікового завдання й оцінювання відповідей на заліку:

Теоретичне питання – 10 балів

Творче питання – 10 балів

Тести – 20 балів (10 тестових завдань x 2 бали)

За бажанням здобувач має можливість обрати тестову форму залікового завдання (білет містить 20 тестових завдань, здобувач одержує 2 бали за кожну вірну відповідь)

УВАГА! У разі використання заборонених джерел на заліку здобувач на вимогу викладача залишає аудиторію та одержує загальну нульову оцінку (0).

У разі настання / подовження дії **обставин непереборної сили** (в тому числі запровадження жорстких карантинних обмежень в умовах пандемії з заборонаю відвідування ЗВО) здобувачам вищої освіти денної форми навчання надається можливість скласти залік **в тестовій формі** (білет містить 20 тестових завдань, здобувач одержує 2 бали за кожну вірну відповідь) **дистанційно на платформі Moodle** в дистанційному курсі «Інформаційна безпека та інформаційні війни», режим доступу: <https://dist.karazin.ua/moodle/course/view.php?id=3884> .

Усний виступ та виконання письмового завдання, тестування	Критерії оцінювання
7-8	Студент у повному обсязі володіє навчальним матеріалом; виявляє творчі здібності; здатен самостійно ставити та вирішувати завдання; самостійно знаходити та використовувати матеріал; вільно самостійно та аргументовано викладає його під час усних виступів та письмових відповідей; глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу; демонструє вміння самостійно робити висновки; студент активно працює протягом семінарського заняття; впевнено відповідає на додаткові запитання; відповідь обов'язково супроводжується інформативною презентацією.
	Відповідь студента є правильною, обґрунтованою, логічною, містить аналіз і систематизацію; зроблені аргументовані висновки; студент активно працює протягом усього семінарського заняття; демонструє глибоке оволодіння лекційним матеріалом; здатний висловити власне ставлення до альтернативних міркувань з
6	конкретної проблеми, проявляє вміння самостійно та аргументовано викладати матеріал, використовуючи при цьому обов'язкову та додаткову літературу; студент активно працює протягом семінарського заняття; впевнено відповідає на додаткові запитання; відповідь супроводжується презентацією.

5	Студент достатньо повно володіє навчальним матеріалом; обґрунтовано його викладає під час усних виступів та письмових відповідей; розкриває зміст теоретичних питань, використовуючи при цьому обов'язкову літературу; вміє знаходити джерело інформації та аналізувати її, ставити та розв'язувати завдання; самостійно оцінює життєві явища і факти, виявляючи особисту позицію щодо них; відповідь супроводжується презентацією; під час відповідей на додаткові запитання мають місце деякі неточності.
4	В цілому студент володіє навчальним матеріалом, викладає його основний зміст, але без глибокого всебічного аналізу, обґрунтування та аргументації; без використання необхідної літератури, допускаючи при цьому окремі суттєві неточності; студент припускається помилок, відповідаючи на додаткові питання; відповідь супроводжується презентацією, в оформленні якої присутні серйозні помилки.
3	Студент не в повному обсязі володіє навчальним матеріалом; студент в цілому оволодів суттю питань з даної теми, втім, відсутні глибокий та всебічний аналіз представленого матеріалу, а також його обґрунтування та аргументація; дає неповні відповіді на запитання, припускається грубих помилок при висвітленні теоретичного матеріалу
2	Відповідь відтворює основні положення навчального матеріалу на рівні запам'ятовування без достатнього розуміння; фрагментарно, поверхово (без аргументації та обґрунтування) викладає їх зміст під час усних виступів та письмових відповідей; недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому неточності; відповіді на запитання містять логічні та фактографічні помилки; відповідь не супроводжується презентацією
1	Студент демонструє фрагментарні знання; не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки; відповідь не супроводжується презентацією.

9. Схема нарахування балів

Поточний контроль, самостійна робота, індивідуальні завдання											Залікова робота	Сума
Розділ 1				Розділ 2				КР	ІЗ	Разом		
T1	T2	T3	T4	T5	T6	T7	T8					
6	7	7	8	8	8	8	8	-	-	60	40	100

Критеріями оцінювання знань за поточний контроль є успішність освоєння знань та набутих навичок на лекціях та семінарських заняттях, що включає систематичність їх відвідування, здатність студента засвоювати категорійний апарат, навички узагальненого мислення, логічність та повноту викладання навчального матеріалу, навички творчо підходити до вирішення поставлених завдань, активність роботи на семінарських заняттях, рівень знань за результатами опитування на семінарських заняттях, самостійне опрацювання тем у цілому чи окремих питань.

Розрахункова шкала для оцінювання роботи здобувачів за поточним контролем:

Схема нарахування балів за одне теоретичне питання залікового білету:

- 9-10 балів - здобувач цілком і всебічно розкрив сутність питання, вільно оперує поняттями і термінологією, демонструє глибокі знання джерел, має власну точку зору стосовно відповідних питань і може аргументовано її доводити;

- 7-8 балів - здобувач розкрив сутність питання, вільно оперує поняттями і термінологією, але спостерігаються деякі упущення при відповідях на питання та неточні обґрунтування;

- 5-6 балів - здобувач розкрив питання у загальних рисах, розуміє їхню сутність, намагається робити висновки, але слабо орієнтується в джерелах, припускається помилок, матеріал викладає нелогічно;

- 0-4 балів - здобувач не розкрив питання навіть у загальних рисах, не розуміє його сутності, не орієнтується в джерелах, припускається грубих помилок, матеріал викладає нелогічно.

Набрана кількість рейтингових балів є основою для оцінки за національною шкалою. Шкала оцінювання наведена нижче.

Шкала оцінювання

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

10. Рекомендована література

Основні законодавчі та нормативно-правові акти

1. Конституція України // Урядовий кур'єр, 13 липня 1996 р.

(Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141)

{Із змінами, внесеними згідно із Законами

[№ 2222-IV від 08.12.2004](#), ВВР, 2005, № 2, ст.44

[№ 2952-VI від 01.02.2011](#), ВВР, 2011, № 10, ст.68

[№ 586-VII від 19.09.2013](#), ВВР, 2014, № 11, ст.142

[№ 742-VII від 21.02.2014](#), ВВР, 2014, № 11, ст.143

[№ 1401-VIII від 02.06.2016](#), ВВР, 2016, № 28, ст.532

[№ 2680-VIII від 07.02.2019](#), ВВР, 2019, № 9, ст.50

[№ 27-IX від 03.09.2019](#), ВВР, 2019, № 38, ст.160}

2. Закон України “Про основи національної безпеки України”//

Урядовий кур'єр, 30 липня 2003 р. (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241)

{Із змінами, внесеними згідно із Законами

[№ 522-IX від 04.03.2020](#), ВВР, 2020, № 34, ст.241

[№ 808-IX від 17.07.2020](#)

[№ 912-IX від 17.09.2020](#)

[№ 1357-IX від 30.03.2021](#), ВВР, 2021, № 29, ст.234

[№ 1702-IX від 16.07.2021](#) - вводиться в дію з [01.01.2022](#)}

3. Закон України “Про державну таємницю” від 21.01.1994 // Відомості Верховної Ради України, 1994, № 16. – Ст. 93. (Відомості Верховної Ради України (ВВР), 1994, № 16, ст.93)

{Вводиться в дію Постановою ВР

[№ 3856-XII від 21.01.94](#), ВВР, 1994, № 16, ст.94}

{В редакції Закону

[№ 1079-XIV від 21.09.99](#), ВВР, 1999, № 49, ст.428}

{Із змінами, внесеними згідно із Законами

[№ 1169-VII від 27.03.2014](#), ВВР, 2014, № 20-21, ст.746

[№ 1170-VII від 27.03.2014](#), ВВР, 2014, № 22, ст.816

[№ 374-VIII від 12.05.2015](#), ВВР, 2015, № 28, ст.245

[№ 576-VIII від 02.07.2015](#), ВВР, 2015, № 36, ст.360

[№ 1798-VIII від 21.12.2016](#), ВВР, 2017, № 7-8, ст.50

[№ 2509-VIII від 12.07.2018](#), ВВР, 2018, № 35, ст.267

[№ 440-IX від 14.01.2020](#), ВВР, 2020, № 28, ст.188

[№ 808-IX від 17.07.2020](#)

[№ 912-IX Від 17.09.2020](#)

4. Закон України “Про інформацію” // Відомості Верховної Ради, 1992, № 48. – Ст. 650 – 651. **Відомості Верховної Ради України (ВВР), 1992, № 48, ст.650)**

{Вводиться в дію Постановою ВР

[№ 2658-XII від 02.10.92](#), ВВР, 1992, № 48, ст.651}

{Офіційне тлумачення до Закону див. в Рішенні Конституційного Суду [№ 5-зп від 30.10.97](#)}

{Із змінами, внесеними згідно із Законами {Із змінами, внесеними згідно із Законами

[№ 317-VIII від 09.04.2015](#), ВВР, 2015, № 26, ст.219

[№ 1405-VIII від 02.06.2016](#), ВВР, 2016, № 28, ст.533

[№ 1774-VIII від 06.12.2016](#), ВВР, 2017, № 2, ст.25

[№ 2704-VIII від 25.04.2019](#), ВВР, 2019, № 21, ст.81

[№ 324-IX від 03.12.2019](#), ВВР, 2020, № 11, ст.63

[№ 720-IX від 17.06.2020](#), ВВР, 2020, № 47, ст.408

[№ 692-IX від 16.06.2020](#), ВВР, 2020, № 43, ст.371}

5. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.1994 // Відомості Верховної Ради України, 1994, № 31. – Ст. 286, із змінами 2005 р.

6. Закон України “Про телекомунікації” від 18.11.2003 // Відомості Верховної Ради України, 2004, № 12. – Ст. 155, із змінами 2004 р.

7. УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №447/2021. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" // <https://www.president.gov.ua/documents/4472021-40013>

Основна література

1. Каплін О.Д. Дистанційний курс «Інформаційна безпека та інформаційні війни» URL: <https://dist.karazin.ua/>
2. Каплін О.Д., Гончарова О.А Мюнхенська конференція з безпеки 2020 р.: Ключові положення основної доповіді, їх дискусійні обговорення і актуальний розвиток подій // Стратегічні напрями зовнішньої політики Європейського Союзу: матеріали III Міжнародної науково-практичної конференції (м. Харків, 16 квітня 2020 року). Х. : ХНУ імені В. Н. Каразіна, 2020. С.125–132.
3. Арквіллі, Дж. Мережі і мережні війни: майбутнє терору, злочинності та бойових дій / Дж. Арквіллі. – К.: Києво-Могилянська академія, 2008. – 350 с.
4. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я. К.: МОУ, 2012, 508 с.
5. Бурячок В.Л., Толубко В.Б., Хорошко В.О., Толюпа С.В. Інформаційна та кібербезпека: соціотехнічний аспект: Підручник. – К.: ДУТ, 2015. – 288 с
6. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навчальний посібник / за заг. ред. В. О. Жадька ; ред.-упор. : О. І. Харитоненко, Ю. С. Полтавець. – Київ : Вид-во НПУ імені М. П. Драгоманова, 2018. – 356 с.
7. Горбулін В.П., Додонов О.Г., Ланде Д.В. [Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія](#). – К. : Інтертехнологія, 2009. – 164 с.
8. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. – Житомир: ЖНАЕУ, 2016. – 636 с.
9. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони. Підручник. – Одеса.: ОНАЗ, 2018 – 228 с.
10. Інформаційні виклики гібридної війни: контент, канали, механізми протидії : аналіт. доп. / за заг. ред. А. Баровської – К. : НІСД, 2016. – 109 с.
11. Історія інформаційно-психологічного протиборства : Підручник [Текст] / [Я. М. Жарков, Л. Ф. Компанцева, В. В. Остроухов та ін.]. – К. : Наук.-вид. відділ НА СБ України, 2012. – 212 с.
12. Куйбіда В. С., Пасічник В. М. Засади державної політики національної безпеки України / за заг. ред. В. С. Куйбіди. Київ: НАДУ, 2020. 488 с.
13. [Курбан О. В. Теорія інформаційної війни: базові основи, методологія та понятійний апарат](#) // Наук. журнал «Science Rise».– 2015.– № 11(1). – С. 95-100.

14. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі [Текст]: Навчальний посібник / О.В.Курбан. – Київ: ВІКНУ, 2016. – 286 с.
15. Ларина Е.С., Овчинский В.С. Кибервойны XXI века. – М.: Книжный мир, 2014. – 352 с.
16. Ларина Е.С., Овчинский В.С. Covid-19: предчувствие апокалипсиса. Хроника океанной пандемии. – М.: Книжный мир, 2020. – 448 с.
17. Лісовський П.М., Лісовська Ю.П. Національна безпека України. К.: Ун-т «Україна», 2020. 292 с.
18. Магда Є. Гібрида війна. Вжити і перемогти [Текст] / Є.Магда. – Київ: Віват, 2015. – 304 с..
19. Матвейчев, О. Информационные войны XXI века. "Мягкая сила" против атомной бомбы / О. Матвейчев. – М.: Книжный мир, 2016. – 353 с.
20. Пасічник В. М. Формування державної політики національної безпеки України на засадах української національної ідеї. Київ : Вид-во ВАДНДУ, 2016. 429 с.;
21. Почепцов Г. Сучасні інформаційні війни [Текст] / Георгій Почепцов. Вид. 2-ге, допов. Київ : Києво-Могилян. акад., 2016. 502 с.
22. Почепцов, Г. Виртуальные войны. Фейки [Текст] / Георгий Почепцов. Харьков : Фолио, 2019. 506 с
23. Рибальський О.В. Основи інформаційної безпеки. Підручник для курсантів ВНЗ МВС України / Рибальський О.В., Смаглюк В.М., Хахановський В.Г. – К.: НАВС, 2013. – 255 с.
24. Сенченко М. І. Латентна світова інформаційна війна.– К.: ФОП Стебеляк, 2014. – 384 с.
25. Стругацький Василь. Маніпулятивні практики на тлі гібридної війни. Філософський аналіз. – Київ: ФОП Халіков Р.Х., 2018. – 166 с.
26. Харченко І.М., Сапогов С.О., Шамраєва В.А., Новікова Л.В. Основні засоби інформаційного протистояння та інформаційної війни як явища сучасного міжнародного політичного процесу // Вісник Харківського національного університету імені В.Н. Каразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм». 2017. Випуск 6. С.77–81.
27. Шмідт, Э., Коен Д. Новый цифровой мир. Переклад з англ. — Львів: Літопис, 2015. — 368 с.

Допоміжна література

1. Абакумов В.М. Правове регулювання протидії інформаційним війнам в Україні. Дис. ... канд. юрид. наук.– Харків, 2010.– 213 с.
2. Бжезінський Збігнєв. [Стратегічне бачення: Америка і криза світової влади](#) / Перекл. з англійської Г. Лелів. – Львів, [«Літопис»](#), 2012. – 168 с.
3. Верголяс О.О. Спеціальні інформаційні операції як інструмент геополітичних змін. Юридичний бюлетень : наук. журн. – Одеса, ОДУВС, 2019. Вип. 9 (9). С. 16-23.
4. Верголяс О.О. Правове забезпечення спеціальних інформаційних операцій. Дис. Канд. Юрид. наук (доктора філософії). – НДІП НАПрН України, Київ, 2020.– 24 с.
5. Домарев В. В. Інформаційна зброя: принципи дії та основні види [Електронний ресурс] / В. В. Домарев // Секьюрити: [сайт]. - Режим доступу: <http://www.security.ukrnet.net/modules/sections/index.php?op=viewarticle&artid=72> 9.
6. Зеленін В.В. По той бік правди: нейролінгвістичне програмування як зброя інформаційно-пропагандистської війни / В.В. Зеленін. – Вінниця: Віндрук, 2015. – 384 с.
7. Золотухін Д. Ю. [Біла книга спеціальних інформаційних операцій проти України 2014 – 2018](#). – К.: «Мега-прес груп», 2018. – 384 с.
8. Исторические аспекты гибридной войны (в американском измерении) [Електронний ресурс] // Борисфен Интел [сайт]. - Режим доступа: <http://bintel.com.ua/ru/article/10-AmericanHybridWar/>
9. Карпчук Н.П. Міжнародна інформація та суспільні комунікації: навч. посіб. для студ. закл. вищ. освіти / Н. П. Карпчук. Луцьк, 2018. 514 с.
10. Коровин В. Третья мировая сетевая война [Текст] / В.Коровин. – СПб.: Питер. 2014. – 352 с.

11. [Курбан О. В. Сучасні інформаційні війни в соціальних онлайн-мережах](#) // Наук. збірник «Інформаційне суспільство». – 2016. – Вип. 23. – С. 85-90.
12. Манойло А.В. Информационные войны и психологические операции. М.: Горячая линия, 2018. – 496 с.
13. Мітін В. І. Інформаційний тероризм на сучасній міжнародній арені / В. І. Мітін // Інтернаука : міжнародний науковий журнал. – 2017. – № 2 (24). – С. 65-68.
14. Операции информационно-психологической войны. Энциклопед. Словарь-справочник. 2-е изд. – М.: Горячая линия, 2019. – 495 с.
15. Панарин И.Н. Гибридная война: теория и практика. – М., 2017. – 404 с.
16. Померанцев Питер. Это не пропаганда. Хроники мировой войны с реальностью. Перевод с англ. М., 2020. – 288 с.
17. Руднєва А. О. Інформаційні війни як фактор впливу на політичну культуру в сучасній Україні. Авт. Дис. ... канд. політ. наук. – Київ, 2014. – 21 с.
18. Смалько О.А. Захист інформаційних ресурсів: Монографія. Кам'янець-Подільський: ПП Буйницький О.А., 2011, 704 с.
19. Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международ. изд. центр «Этносоциум», 2017. 124 с
20. Ульянова Н.Н. Информационные войны в печатных СМИ на примере Косовского этнического конфликта: сравнительный анализ публикаций "Российской газеты" и "The Washington Post" 2008-2013 гг.: Автореф. дис. ... канд. филолог. наук / РУДН. – М., 2015. – 21 с.
21. Armistead L. Information operations matters. Best practices. – Washington, 2010.
22. Dando M. Neuroscience and the future of chemical-biological weapons. - New York etc., 2015.
23. Ideas as weapons. Influence and perception in modern warfare. Ed. by GJ David Jr., TR McKeldin III. – Washington, 2009.
24. Influence warfare. How terrorists and governments fight to shape perceptions in a war of ideas. Ed. by JJF Forest. – Westport–London, 2009.
25. Information operations. Warfare and the hard reality of soft power. Ed. By L. Armistead. – Washington, 2004.
26. Information warfare. Separating hype from reality. Ed. by L. Armistead. – Washington, 2007.
27. Thaler R.H. Misbehaving. The making of behavioral economics. - New York, 2015.
28. Thomas TL Dragonbytes. Chinese information-war theory and practice. – Fort Leavenworth, 2004.
29. "The New Digital Age: Reshaping the Future of People, Nations and Business" by Eric Schmidt, Jared Cohen. New York, 2014.
30. *The Inevitable: Understanding the 12 Technological Forces that Will Shape Our Future.* Front Cover. Kevin Kelly. – Viking, 2016.
31. Milton Bearden. *Secrets and Lies: Information Warfare During The Cold War and Today* // *The National Interest*. August 31, 2020.

Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. Верховна Рада України - www.zakon1.rada.gov.ua.
2. Міністерство закордонних справ - <http://mfa.gov.ua/ua>
3. Міністерство юстиції - <https://minjust.gov.ua/ua>
4. Конституційний Суд України - <http://www.ccu.gov.ua/uk/index>
5. Організація Об'єднаних Націй - <http://www.un.org/>
6. Європейський суд з прав людини - <http://echr.coe.int/>
7. Європейський союз - <http://eeas.europa.eu/>
8. Організація з безпеки та співробітництва в Європі - <http://www.osce.org/>
9. Рада Європи - <http://www.coe.int/web/portal/home>
10. Управління Верховного комісара ООН з прав людини - <http://www.ohchr.org/>
11. Національна парламентська Бібліотека України - <http://www.nplu.org/>
12. Національна бібліотека України імені В. І. Вернадського - www.nbuv.gov.ua

13. Київська центральна міська публічна бібліотека ім. Лесі Українки - <http://lucl.lucl.kiev.ua>
14. Центральна наукова бібліотека Харківського національного університету ім. В.Н. Каразіна - <http://www.univer.kharkov.ua>
15. Харківська державна наукова бібліотека ім. В. Г. Короленка - <http://korolenko.kharkov.com>

12. Особливості навчання за денною формою в умовах подовження дії обставин непоборної сили (в тому числі запровадження карантинних обмежень через пандемію)

В умовах дії карантинних обмежень освітній процес в університеті здійснюється за змішаною формою навчання, а саме:

- дистанційно (за затвердженим розкладом занять) на платформі Zoom проводяться всі лекційні заняття;
- дистанційно на платформі Moodle (<https://dist.karazin.ua/moodle/course/view.php?id=3884>) проводяться практичні (семінарські), індивідуальні заняття та консультації, контроль самостійної роботи;
- аудиторно (за затвердженим розкладом занять) проводяться 10% практичних та семінарських занять у навчальних групах кількістю до 20 осіб з урахуванням відповідних санітарних і протиепідемічних заходів.

Складання підсумкового семестрового контролю: в разі запровадження жорстких карантинних обмежень з заборотою відвідування ЗВО здобувачам денної форми навчання надається можливість (за заявою, погодженою деканом факультету) скласти **залік в тестовій формі дистанційно на платформі Moodle** в дистанційному курсі «Інформаційна безпека та інформаційні війни» режим доступу: <https://dist.karazin.ua/moodle/course/view.php?id=3884> .