

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

Антоніант ТЕМЕЛЕЙМОНОВ

2020 р.

Робоча програма навчальної дисципліни

Міжнародна інформаційна безпека

рівень вищої освіти: другий (магістерський)

галузь знань: 29 «Міжнародні відносини»

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

освітня програма: «Міжнародна інформаційна безпека»

вид дисципліни: обов'язкова

факультет міжнародних економічних відносин та туристичного бізнесу

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

«28» серпня 2020 року, протокол № 1

РОЗРОБНИКИ ПРОГРАМИ: канд. юрид. наук., доцент кафедри Олена ДОЦЕНКО

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

Протокол від «26» серпня 2020 року № 1

Завідувач кафедри

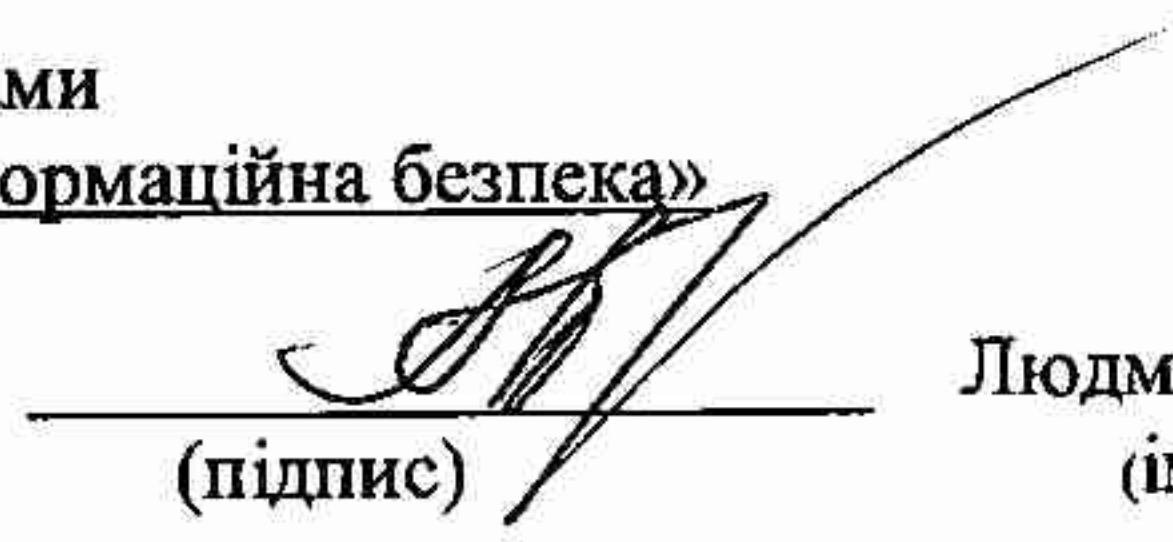

(підпис)

Людмила НОВІКОВА
(ім'я та прізвище)

Програму погоджено з гарантом освітньо-професійної програми
«Міжнародна інформаційна безпека»
назва освітньої програми

Гарант освітньо-професійної програми

«Міжнародна інформаційна безпека»

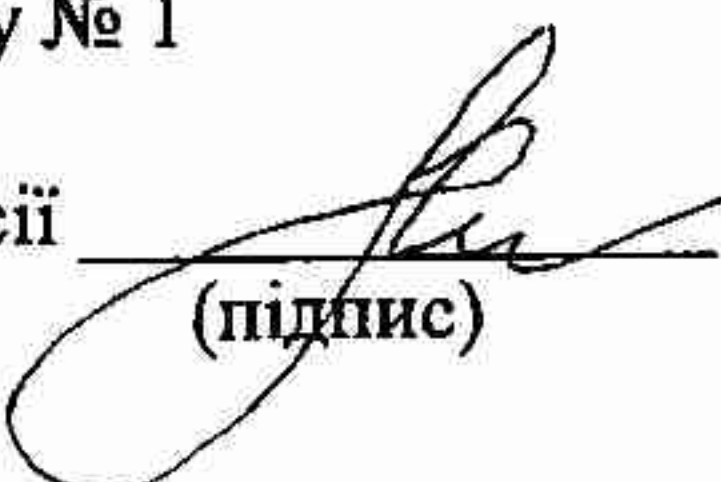

(підпис)

Людмила НОВІКОВА
(ім'я та прізвище)

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

Протокол від «28» серпня 2020 року № 1

Голова навчально-методичної комісії


(підпис)

Лариса ГРИГОРОВА-БЕРЕНДА
(ім'я та прізвище)

ВСТУП

Програму навчальної дисципліни «Міжнародна інформаційна безпека» складено відповідно до освітньо-професійної програми «Міжнародна інформаційна безпека» підготовки магістра за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії».

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни полягає у формуванні у здобувачів базових знань щодо основних понять, методів, підходів та тенденцій міжнародної інформаційної безпеки, а також практичних умінь та навичок визначення місця, особливостей і основних тенденцій трансформації безпеки в сучасній світовій політиці у зв'язку із загальною інформатизацією і формуванням інформаційного суспільства, правильного тлумачення та застосування міжнародних нормативно-правових актів, необхідних для їх майбутньої трудової діяльності як фахівців у сфері міжнародної інформаційної безпеки.

1.2. Основні завдання вивчення дисципліни:

- формування наступних фахових компетентностей:

ФК 1. Поглиблені знання про природу, динаміку, принципи організації міжнародних відносин, типи та види міжнародних акторів, сучасні тенденції розвитку світової політики.

ФК 3. Здатність аналізувати та прогнозувати міжнародні відносини у різних контекстах, зокрема політичному, безпековому, правовому, суспільному, культурному та інформаційному.

ФК 4. Поглиблені знання про теоретичні та прикладні дослідження міжнародних відносин і світової політики у політичній, економічній, юридичній науках, у міждисциплінарних дослідженнях.

ФК 7. Здатність провадити прикладні аналітичні розробки проблем міжнародних відносин та світової політики, фахово готувати аналітичні матеріали та довідки.

ФК 11. 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	
Обов'язкова	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2-й	-й
Семестр	
3-й	-й
Лекції	
10 год.	- год.
Практичні заняття	
10 год.	- год.
Лабораторні заняття	
- год.	- год.
Самостійна робота	

70 год.	- год.
у т.ч. індивідуальні завдання	
- год.	

2. Заплановані результати навчання

Згідно з вимогами освітньо-професійної програми матриця відповідності освітнього компонента **ВБ 1.6. «Міжнародна інформаційна безпека»**, методів навчання та форм оцінювання, які використовуються, програмним результатам навчання, визначеним освітньо-професійною програмою «Міжнародна інформаційна безпека».

Результати навчання	Методи навчання	Форми оцінювання
ПРН 35 – знання сучасних концепцій та стратегій міжнародної інформаційної безпеки.	Пояснювально-ілюстративний, пояснювально-рецептивний, репродуктивний, проблемний виклад, евристичний, проблемно-пошуковий, дослідницький, метод оволодіння новими знаннями, методи стимулювання інтересу до навчання, методи контролю та корекції за ефективністю навчально-пізнавальної діяльності, а також методи дистанційного навчання та оцінювання на платформах Moodle, Zoom або Google Meet.	Підготовка відповідей за навчальними питаннями теми, усне опитування та навчальні дискусії; виконання тестових завдань; підготовка та захист презентацій доповідей; підготовка тематичних схем; підготовка та захист есе; аналіз наукової статі та нормативних актів та навчальні дискусії за науковою статтею та нормативними актами, групова робота з підготовки питань для колоквіуму, колоквіум.
ПРН 42 – володіти сучасними концепціями та стратегіями міжнародної інформаційної безпеки.	-/-	-/-
ПРН 49 – використовувати сучасні концепції та стратегії міжнародної інформаційної безпеки.	-/-	-/-

3. Тематичний план навчальної дисципліни

Розділ 1. Загальні засади міжнародної інформаційної безпеки

Тема 1. Концепція інформаційного протистояння в міжнародних відносинах.

Інформаційний чинник конфліктів у сучасних міжнародних відносинах. Поняття та зміст інформаційного протистояння. Форми ведення інформаційного протистояння (інформаційна експансія, інформаційна агресія, інформаційна війна).

Тема 2. Теоретичні засади інформаційної безпеки.

Поняття та види інформаційної безпеки. Сучасні інформаційні загрози. Поняття та види інформаційної зброї. Моделі системи глобальної інформаційної безпеки.

Тема 3. Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру.

Вплив інформаційної революції на систему міжнародної безпеки. Діяльність ООН у сфері міжнародної інформаційної безпеки. Роль Всесвітнього саміту з питань інформаційного суспільства у розвитку міжнародного співробітництва у сфері інформаційної безпеки. Роль міжнародної організації кримінальної поліції (Інтерпол) у сфері міжнародної інформаційної безпеки.

Тема 4. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки.

Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки європейських держав. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки американських держав. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки держав Азії та Азіатсько-Тихоокеанського регіону.

4. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с. р.		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Загальні засади інформаційної безпеки у міжнародних відносинах												
Тема 1. Концепція інформаційного протиборства в міжнародних відносинах	22	2	2	-	-	18	-	-	-	-	-	-
Тема 2. Теоретичні засади інформаційної безпеки	18	2	2	-	-	14	-	-	-	-	-	-
Тема 3. Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру	18	2	2	-	-	14	-	-	-	-	-	-
Тема 4. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки	32	4	4	-	-	24	-	-	-	-	-	-
Усього годин	90	10	10	-	-	70	-	-	-	-	-	-

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Концепція інформаційного протиборства в міжнародних відносинах	2
2	Теоретичні засади інформаційної безпеки	2
3	Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру	2
4	Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки	4
	Разом	10

5. Завдання для самостійної роботи

№ з/п	Назва теми та зміст самостійної роботи	Кількість годин
1	Тема 1. Концепція інформаційного протиборства в міжнародних відносинах. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття; підготувати презентації доповідей на визначену тему (на вибір); підготувати письмово тематичну схему; ознайомитися та проаналізувати наукову статтю; підготувати есе на визначену тему.	18
2	Тема 2. Теоретичні засади інформаційної безпеки. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття; підготувати презентації доповідей на визначену тему (на вибір); підготувати письмово тематичну схему; підготувати есе на визначену тему (на вибір).	14
3	Тема 3. Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття; підготувати презентації доповідей на визначену тему (на вибір); підготувати письмово тематичну схему; підготувати есе на визначену тему.	14
4	Тема 4. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття; підготувати презентації доповідей на визначену тему (на вибір); підготувати письмово тематичну схему; ознайомитися та проаналізувати нормативні акти; підготувати есе на визначену тему; поділитися на дві групи та підготувати питання здобувачам іншої групи за всіма темами курсу для колоквіуму.	24
	Разом	70

7. Індивідуальні завдання

Не передбачено.

8. Методи контролю

Поточний контроль знань здобувачів проводиться на *практичному занятті у формі усного опитування та навчальної дискусії, виконання тестових завдань, захисту презентацій доповідей, навчальних дискусій за науковою статтею та нормативними актами, захисту есе, колоквіуму* тощо.

Сума балів за виконання завдань на практичному занятті складає:

Тема 1 – 3,5 бали: (захист презентацій доповідей – 1 бал; навчальна дискусія за науковою статтею – 1,5 бали; захист есе – 1 бал).

Тема 2 – 3 бали: (захист презентацій доповідей – 1 бал; виконання тестових завдань – 1 бал; захист есе – 1 бал).

Тема 3 – 3 бали: (захист презентацій доповідей – 1 бал; виконання тестових завдань – 1 бал; захист есе – 1 бал).

Тема 4 – 12 балів: (захист презентацій доповідей – 2 бали; виконання тестових завдань – 1 бал; навчальні дискусії за нормативними актами – 3 бали; захист есе – 1 бал; колоквіум – 5).

Поточний контроль *самостійної роботи здобувачів проводиться у формі підготовки відповідей за навчальними питаннями теми, підготовки презентацій доповідей, підготовки тематичних схем, підготовки есе, аналізу статей, аналізу нормативних актів, групової роботи з підготовки питань для колоквіуму.*

Сума балів за виконання завдань для самостійної роботи здобувачів складає:

Тема 1 – 8,5 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; підготовка презентацій доповідей – 2 бали; підготовка тематичної схеми – 1 бал; аналіз статті – 1,5 бали; підготовка есе – 2 бали.

Тема 2 – 7 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; підготовка презентацій доповідей – 2 бали; підготовка тематичної схеми – 1 бал; підготовка есе – 2 бали.

Тема 3 – 7 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; підготовка презентацій доповідей – 2 бали; підготовка тематичної схеми – 1 бал; підготовка есе – 2 бали.

Тема 4 – 16 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; підготовка презентацій доповідей – 4 бали; підготовка тематичної схеми – 1 бал; аналіз нормативних актів – 3 бали; підготовка есе – 2 бали; групова робота з підготовки питань до колоквіуму – 4.

Загальна сума балів за виконання завдань для самостійної роботи та роботу на практичних заняттях може сягати 60 балів.

Підсумковий семестровий контроль проводиться у формі заліку. Вміст залікового білета й оцінювання відповідей на заліку: 40 тестових завдань. Максимальна кількість балів – 40 (правильна відповідь на 1 тестове завдання = 1 бал).

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

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 та заочної форм навчання надається можливість скласти залік **у такій самій формі дистанційно на платформі Moodle** в дистанційному курсі «Міжнародна інформаційна безпека».

9. Схема нарахування балів

Поточний контроль, самостійна робота				Разом	Залікова робота	Сума
Розділ 1						
T1	T2	T3	T4	60	40	100
12	10	10	28			

T1, T2 ... – теми розділів.

Критерії оцінки успішності та результатів навчання

Критеріями оцінювання знань за поточний контроль є рівень засвоєння знань та набуття навичок на лекціях та практичних заняттях, що включає систематичність їх відвідування, здатність здобувача засвоювати категорійний апарат, вміння орієнтуватися у сучасних подіях в світі і державі, навички узагальненого мислення, логічність та повноту засвоєння навчального матеріалу, навички творчого підходу до вирішення поставлених завдань, активність роботи на практичних заняттях, рівень знань за результатами опитування на практичних заняттях, самостійне опрацювання тем в цілому чи окремих питань.

Розрахункова шкала для оцінювання роботи здобувачів за поточним контролем.

Кількість балів	Критерії оцінювання
52–60	Систематичне відвідування лекцій та практичних занять, відсутність пропусків занять без поважної причини, відпрацювання тем практичних занять, пропущених з поважної причини, виконання завдань до кожного практичного заняття, висока активність роботи на практичному занятті, засвоєння всього обсягу матеріалу, повні та обґрунтовані відповіді при виконанні завдань, здатність визначення теоретичних питань, на які розраховані завдання, уміння сформулювати своє ставлення до певної проблеми теми, вміння мислити абстрактно і узагальнено, здатність публічно представити матеріал.
44–51	Систематичне відвідування лекцій та практичних занять, відсутність пропусків занять без поважних причин, відпрацювання тем практичних занять, пропущених з поважної причини, виконання завдань до кожного практичного заняття, висока активність роботи на практичному занятті, засвоєння всього обсягу матеріалу, повні та обґрунтовані відповіді з несуттєвими помилками при виконанні завдань, здатність визначення теоретичних питань, на які розраховані завдання, уміння сформулювати своє ставлення до певної проблеми теми, здатність публічно представити матеріал.
37–43	Наявність пропущених лекцій та практичних занять, відпрацювання тем пропущених практичних занять, виконання завдань до кожного практичного заняття, активна робота на практичних заняттях, засвоєння основних положень курсу, допущення декількох незначних помилок при виконанні завдань, здатність визначення теоретичних питань, на які розраховані завдання, здатність публічно представити матеріал.
29–36	Наявність пропущених лекцій та практичних занять, відпрацювання тем пропущених та практичних занять, епізодична відсутність виконання завдань,

	участь у роботі на практичних заняттях, засвоєння окремих положень матеріалу, неповні відповіді при виконанні завдань, складності при визначенні теоретичних питань, на які розраховані завдання, здатність публічно представити матеріал.
21–28	Несистематичне відвідування лекцій та практичних занять, відсутність на заняттях без поважних причин, наявність декількох невідпрацьованих тем пропущених практичних занять, епізодична відсутність виконаних завдань, участь у роботі на практичних заняттях, засвоєння окремих положень матеріалу тем змістовного розділу, неповні відповіді, допущення помилок при виконанні завдань, великі складності при визначенні теоретичних питань на які розраховані завдання, невпевнені навички публічного представлення матеріалу.
13-20	Епізодичне відвідування лекцій та практичних занять, відсутність на заняттях без поважної причини, наявність невідпрацьованих тем пропущених лекцій та практичних занять, епізодична відсутність виконаних завдань, пасивна робота на практичних заняттях (участь у роботі останніх лише за наявності стимулу з боку викладача), наявність певного уявлення щодо матеріалу тем змістовного розділу, неповні відповіді, допущення значної кількості помилок при виконання завдання, невміння визначити теоретичні питання, на які розраховано завдання, невпевнені навички публічного представлення матеріалу.
6-12	Систематичні пропуски лекцій та практичних занять без поважних причин, наявність невідпрацьованих тем пропущених лекцій та практичних занять, систематична відсутність виконаних завдань, пасивність у роботі на практичних заняттях, неповні, необґрунтовані відповіді, допущення істотних помилок при виконанні завдань, нездатність визначити теоретичні питання, на які розраховані завдання.
0-5	Систематичні пропуски лекцій та практичних занять без поважних причин, теми пропущених лекцій та практичних занять не відпрацьовані, систематична відсутність виконаних завдань, пасивність у роботі на практичних заняттях, відсутність знань, неповні, необґрунтовані відповіді, допущення істотних помилок при виконанні завдання, нездатність визначити теоретичні питання, на які розраховані завдання, невміння публічно представити матеріал, порушення норм академічної доброчесності при виконанні завдань.

Результати оцінювання роботи здобувачів фіксуються у відповідній відомості.

Здобувачі, які були відсутні на лекції чи практичному занятті або отримали незадовільну оцінку, відпрацьовують пропущене заняття або незадовільну оцінку викладачу у дні його консультацій за графіком, затвердженим кафедрою. Для відпрацювання здобувач зобов'язаний надати індивідуально виконане завдання за темою пропущеного заняття та продемонструвати належний рівень теоретичної підготовки за темою заняття, яке відпрацьовується.

До заліку допускаються здобувачі, які були присутніми не менш ніж на 70% занять з навчальної дисципліни, враховуючи відпрацьовані, та набрали не менш, ніж 25 балів за поточний контроль знань.

Оцінювання знань та умінь здобувачів при підсумковому контролі здійснюється відповідно до наступних критеріїв:

Кількість балів	Критерії оцінювання
40	Здобувач правильно відповів на всі тестові питання.
30	Здобувач правильно відповів на не менш, ніж 75 % тестових питань.

20	Здобувач правильно відповів на не менш, ніж 50 % тестових питань.
10	Здобувач правильно відповів на не менш ніж 25 % тестових питань.
0	Здобувач не відповів на жодне з тестових питань.
Правильна відповідь на одне тестове питання – 1 бал.	

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	
50–69	задовільно	
1–49	незадовільно	не зараховано

10. Рекомендована література

Основна література

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за ред. проф. В. Б. Толубка. Київ: ДУТ, 2015. 288 с.
2. Гапасьва О. Міжнародна інформаційна безпека – ключовий напрям діяльності Шанхайської організації співробітництва: 2006–2017 рр. *Східноєвропейський історичний вісник*. 2017. Вип. 4. С. 155–163.
3. Грицун О. О. Поняття міжнародної інформаційної безпеки: порівняльно-правовий аспект. *Науковий вісник Ужгородського національного університету*. Серія ПРАВО. 2015. Випуск 31. Том 3. С. 123–127. URL: http://www.visnyk-juris.uzhnu.uz.ua/file/No.31/part_3/33.pdf (дата звернення: 20.08.2020).
4. Дерекко В.Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави*. 2015. № 2 (18). С.16–22.
5. Зозуля О. С. Інформаційна зброя як геополітичний чинник та інструмент силової політики. *Державне управління: теорія та практика*. 2013. № 2. С. 82–89. URL: http://nbuv.gov.ua/UJRN/Dutp_2013_2_12 (дата звернення: 20.08.2020).
6. Інформаційна безпека (соціально-правові аспекти) / В. Остроухов, В. Петрик, М. Присяжнюк та ін. ; за ред. Є.Д. Скулиша. К. : КНТ, 2010. 776 с.
7. Карпов О. Н. Можливості використання баз даних Міжнародної організації кримінальної поліції – Інтерпол у протидії тероризму. *Питання інформаційної безпеки*. 2009. № 21. С. 301–306.
8. Кириченко І. О. Співробітництво організації американських держав та Сполучених Штатів Америки у сфері інформаційної безпеки. *Актуальні проблеми міжнародних відносин*. 2010. Випуск 93 (Частина І). С. 160–164.
9. Король А. Інформаційні технології в системі міжнародних відносин: проблема впровадження. *Мультиверсум. Філософський альманах*. 2015. Випуск 3–4 (141–142). С. 59–67.
10. Лапінська Є. І. Інформаційна безпека: поняття, види та ознаки. *Порівняльно-аналітичне право*. 2018. № 6. С. 262–266.
11. Левченко О. В. Класифікація інформаційної зброї за засобами ведення інформаційної боротьби. *Сучасні інформаційні технології у сфері безпеки та оборони*.

2014. № 2. С. 142–146 URL: http://nbuv.gov.ua/UJRN/sitsbo_2014_2_25 (дата звернення: 20.08.2020).

12. Макаренко Є. А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст. *Актуальні проблеми міжнародних відносин*. 2011. Випуск 102 (Частина I). С. 160–164

13. Макаренко Є. Інформаційне протистояння у сучасних міжнародних відносинах. *Міжнародні відносини. Серія «Політичні науки»*. 2017. № 17. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3316/2995 (дата звернення: 20.08.2020).

14. Міжнародна та національна безпека: теоретичні і прикладні аспекти : матер. III Міжнар. наук.-практ. конф. (м. Дніпро, 15 бер. 2019 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2019. 365 с. URL: <https://dduvs.in.ua/wp-content/uploads/files/Structure/science/publish/np2d5.pdf> (дата звернення: 20.08.2020).

15. Петровський О. М., Лівчук С. Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та Українські реалії. *Young Scientist*. 2019. № 12.1 (76.1). С. 55–60.

16. Терещук В. І. Міжнародні комунікації у безпековому дискурсі ООН: наявні і потенційні виклики. *Міжнародні відносини. Серія «Політичні науки»*. 2019. № 21. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3874/3534 (дата звернення: 10.05.2020).

17. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. Підприємництво, господарство і право. 2017. № 10. С. 182–186. URL: <http://pgr-journal.kiev.ua/archive/2017/10/38.pdf> (дата звернення: 20.08.2020).

18. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах Євроінтеграції України: дис. ... докт. юрид. наук: 12.00.07 / ДВНЗ «Ужгородський національний університет. Ужгород, 2019. 487 с.

19. Толубко В. Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : монографія. Київ : НАОУ, 2003. 320 с.

20. Фролова О. М. Роль ООН в системі міжнародної інформаційної безпеки. *Міжнародні відносини. Серія «Політичні науки»*. 2018. № 18–19. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/viewFile/3468/3140 (дата звернення: 20.08.2020).

21. Широкова-Мурараш О. Г., Акчурін Ю. Р. Кіберзлочинність та кібертероризм як загроза інформаційній безпеці: міжнародно-праовий аспект. *Інформація і право*. 2011. № 1(1). С. 76–81. URL: <http://dspace.nbuv.gov.ua/bitstream/handle/123456789/38938/14-Shirokova.pdf?sequence=1> (дата звернення: 20.08.2020).

22. Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2nd ed. Syngress, 2014. 240 p.

23. Giacomello G. Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. 1st ed. Bloomsbury Academic, 2014. 256 p.

24. Overview of Cybersecurity Status in ASEAN and the EU. Sociedade Portuguesa de Inovação (SPI), 2018. 87 p. URL: <https://ec.europa.eu/research/participants/documents/downloadPublic/VndWdmIxYWFBQUVNATc4Y25aWkxISVpLSXRPQjBiK0IHakYrMlNla3JOZGhkaWRNUnRZbTVVBPT0=/attachment/VFEyQTQ4M3ptUWNCZ0ErcVdweUc2Mnlzc0hRQ2gwVWg=> (Last Accessed: 20.08.2020).

25. What is the Difference between Cyber Security and Information Security? *Computer Science Degree Hub*. URL: <https://www.computersciencedegreehub.com/faq/what-is-the-difference-between-cyber-security-and-information-security/> (Last Accessed: 20.08.2019).

Допоміжна література

1. Близнюк А. Гібридна війна XXI століття. Пропаганда як основна складова у політичних, соціальних та етнічних протистояннях. *Інтермарум: історія, політика, культура*. 2015. Вип. 2. С. 390–399.

2. Бойко С. Проблематика международной информационной безопасности на площадках ШОС и БРИКС. *Международная жизнь* : веб-сайт. 23.01.2019. URL: <https://interaffairs.ru/news/show/21480> (дата звернення: 20.08.2020).
3. Валушко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту: дис. ... канд. політ. наук: 23.00.04 / Дипломатична академія України при МЗС України; Чорноморський національний університет імені Петра Могили. Київ, 2018. 210 с.
4. Коломієць О. В. Особливості системи міжнародної безпеки в умовах глобалізації : автореф. дис. ... д-ра політ. наук : 23.00.04 / Нац. ун.-т «Одеська юридична академія». Одеса, 2015. 36 с.
5. Король А. М. Інформаційні чинники демократизації політичної культури у системі міжнародних відносин : дис. ... канд. політ. наук: 23.00.03 / Нац. пед. ун.-т. ім. М. П. Драгоманова. Київ, 2016. 203 с.
6. Любохинець Л. С., Поплавська О. В. Світова практика забезпечення інформаційної безпеки в сучасному глобалізованому середовищі. *Науково-виробничий журнал «Бізнес-навігатор»*. 2017. Випуск 4-1 (43). С. 93–97.
7. Почепцов Г. Г. Сучасні інформаційні війни. Київ: Києво-Могилянська академія, 2015. 498 с.
8. Рижук О. М. Поняття інформаційних та гібридних війн в умовах глобалізації. *Освіта регіону. Політологія. Психологія. Комунікації*. 2016. № 3. С. 84–88. URL: <https://social-science.uu.edu.ua/article/1389> (дата звернення: 20.08.2020).
9. Саприкін О. Інформаційна експансія, інформаційна війна та інформаційна атака у засобах масової інформації на прикладі Євро-2012. *Вісник Книжкової палати*. 2013. Вип. 1. С. 40–43.
10. Сербіна К. Ю. Необхідність реформування безпекового простору у контексті протидії новим викликам безпеці (на прикладі діяльності організації американських держав). *Актуальні проблеми міжнародних відносин*. 2012. Випуск 107 (Частина II). С. 151–161.
11. Сорокін О. Л. Інформаційна безпека та її складові: проблеми визначення концепту. *Держава та право*. 2014. № 8. С. 18–22.
12. Соснін О. В., Воронкова В. Г., Постол О. Є. Сучасні міжнародні системи та глобальний розвиток (соціально-політичні, соціально-економічні, соціально-антропологічні виміри) : навч. посіб. Київ, 2015. 556 с.
13. Чекаленко Л. Про поняття «гібридна війна». *Журнал «Віче»*. 2015. № 5. С. 41–42. URL: http://nbuv.gov.ua/UJRN/viche_2015_5_21 (дата звернення: 20.08.2020).
14. Щепанівський В. Г. Інформаційна безпека як складова сучасного образу України. *Актуальні проблеми міжнародних відносин*. 2011. Випуск 102 (Частина I). С. 219–228.
15. Яцишин М. Ю. Роль міжнародних організацій у протидії кіберзлочинності. *Українське право*. 15.12.2019. URL: https://ukrainepravo.com/international_law/public_international_law/rozmizhnarodnykh-organizatsiy-u-protydyi-kiberzlochynnosti/ (дата звернення: 20.08.2020).
16. About APEC. *Asia-Pacific Economic Cooperation* : веб-сайт. URL: <https://www.apec.org/About-Us/About-APEC> (Last Accessed: 20.08.2020).
17. About CSIRTs Network. *CIRTsNetwork* : web-site. URL: <https://csirtsnetwork.eu/> (Last Accessed: 20.08.2020).
18. About ENISA. *ENISA* : web-site. URL: <https://www.enisa.europa.eu/about-enisa> (Last Accessed: 20.08.2020).
19. About Us. *CERT-EU*. URL: https://cert.europa.eu/cert/plainedition/en/cert_about.html (Last Accessed: 20.08.2020).
20. Collins A. *Contemporary Security Studies*. 3rd ed. United Kingdom: Oxford University Press, 2013. 478 p.
21. Cyber Europe 2020. URL: <https://www.enisa.europa.eu/topics/cyberexercises/cyber-europe-programme/cyber-europe-2020/> (Last Accessed: 20.08.2020).

22. Deutsch M., Coleman P. T., Marcus E. C. The handbook of conflict resolution: theory and practice. 3rd. ed. San Francisco : John Wiley & Sons, 2014. 1264 p.
23. European Cybercrime Centre - EC3. Combating crime in a digital age. URL: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3> (Last Accessed: 20.08.2020).
24. The Shanghai Cooperation Organisation. *The Shanghai Cooperation Organisation* : веб-сайт. URL: http://eng.sectsco.org/about_sco/ (Last Accessed:20.08.2020).
25. Who we are. OAS : веб-сайт. URL: http://www.oas.org/en/about/who_we_are.asp (Last Accessed: 20.08.2020).

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>

11. 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 проводяться практичні, індивідуальні заняття та консультації, контроль самостійної роботи;
- аудиторно (за затвердженим розкладом занять) проводяться 10% практичних та практичних 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 заборною відвідування ЗВО здобувачам денної форми навчання надається можливість (за заявою, погодженою деканом факультету) скласти **залік дистанційно на платформі Moodle** <https://dist.karazin.ua/moodle/login/index.php>

12. Перелік питань до заліку

Заліковий білет містить 40 тестових завдань.

Питання для підготовки:

1. Роль процесів глобалізації та інформатизації у взаємодії суб'єктів міжнародних відносин.
2. Поняття та сутність міжнародного конфлікту.
3. Основні функції міжнародного конфлікту.
4. Методи інформаційно-психологічного впливу у сучасних міжнародних конфліктах.
5. Поняття та зміст інформаційного протиборства.
6. Історичні етапи розвитку інформаційного протиборства.
7. Фактори та умови сучасного ведення інформаційного протиборства.
8. Мета та принципи інформаційного протиборства.
9. Стадії інформаційного протиборства.
10. Поняття, та ознаки інформаційної експансії.
11. Поняття та ознаки інформаційної агресії, її види.
12. Поняття та ознаки інформаційної війни.
13. Основні підходи до визначення поняття «інформаційна безпека».
14. Поняття «міжнародна інформаційна безпека».
15. Класифікації інформаційної безпеки.
16. Поняття інформаційних загроз та їх властивості.
17. Класифікації загроз інформаційній безпеці.
18. Інформаційна злочинність та інформаційний тероризм.
19. Поняття та ознаки інформаційної зброї.
20. Класифікації інформаційної зброї.
21. Моделі системи глобальної інформаційної безпеки.
22. Фактори ефективності системи міжнародної безпеки.
23. Резолюції ГА ООН «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки».
24. Діяльність Спеціальної групи урядових експертів держав-членів ООН в сфері міжнародної інформаційної безпеки.
25. Роль Всесвітнього саміту з питань інформаційного суспільства у розвитку міжнародного співробітництва у сфері інформаційної безпеки.
26. Роль міжнародної організації кримінальної поліції (Інтерпол) у сфері міжнародної інформаційної безпеки.
27. Конвенція Ради Європи про кіберзлочинність 2001 року.
28. Ініціатива «Електронна Європа» (eEurope).
29. Діяльність Агентства ЄС з мереж і інформаційної безпеки (ENISA).
30. Навчання Cyber Europe.
31. Діяльність Команди реагування на надзвичайні ситуації CERT-EU.
32. Діяльність Європейського центру по боротьбі з кіберзлочинністю (EC3).
33. Директива 2016/1148 про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС 2016 року (NIS Directive).
34. Інструменти забезпечення інформаційної безпеки в рамках АТЕС.
35. Результати самітів міністрів АТЕС у сфері телекомунікацій та інформації.
36. Інструменти забезпечення інформаційної безпеки в рамках АСЕАН.
37. Регіональний форум АСЕАН з питань безпеки.
38. Інструменти забезпечення інформаційної безпеки в рамках ШОС.
39. Інструменти забезпечення інформаційної безпеки в рамках ОАД.
40. Роль Міжамериканської комісії з питань зв'язку (CITEL) у забезпеченні інформаційної безпеки.