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

“ 31 ” серпня 2021 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

2021 / 2022 навчальний рік

2

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

"27" серпня 2021 року, протокол № 1

Розробники програми:
Доценко О. М., к.ю.н., доцент кафедри міжнародних відносин, міжнародної інформації та безпеки

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

Протокол від "_26___" серпня 2021 року, протокол № _1___

Завідувачка кафедри _____ Людмила НОВИКОВА
(підпис) (прізвище та ініціали)

Програму погоджено з гарантами освітніх програм.

Гарант освітньої програми «Міжнародна інформаційна безпека» другого (магістерського) рівня _____ Людмила НОВІКОВА
(підпис) (ім'я та прізвище)

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

Протокол № 1 від "26" серпня 2021 року

Голова науково-методичної комісії факультету міжнародних економічних відносин та туристичного бізнесу
_____ Лариса ГРИГОРОВА-БЕРЕНДА
(підпис) (ім'я та прізвище)

ВСТУП

Програма навчальної дисципліни **“Міжнародна інформаційна безпека”** складена відповідно до освітньо-професійної програми **«Міжнародна інформаційна безпека»** підготовки **магістра** за спеціальністю **291 «Міжнародні відносини, суспільні комунікації та регіональні студії»**

1. МЕТА ТА ЗАВДАННЯ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1.1. Метою дисципліни є: формування 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.

Вивчення навчальної дисципліни передбачає формування та розвиток у здобувачів вищої освіти компетентностей та програмних результатів навчання відповідно до ОПП.

1.2. Основним завданням вивчення дисципліни “Міжнародна інформаційна безпека” є:

- **формування наступних загальних компетентностей**

ЗК1. Здатність проводити дослідження на відповідному рівні.

ЗК3. Вміння виявляти, ставити та вирішувати проблеми.

ЗК5. Здатність генерувати нові ідеї (креативність).

ЗК12. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

- **формування наступних фахових компетентностей**

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

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

СК7. Здатність здійснювати прикладні аналітичні дослідження проблем міжнародних відносин та світової політики, суспільних комунікацій, регіональних студій, професійно готувати аналітичні матеріали та довідки.

СК14. Здатність оцінювати зміст та основні напрями діяльності міжнародних організацій в сфері безпеки та сучасних стратегій забезпечення міжнародної інформаційної безпеки.

СК15. Здатність виявляти та аналізувати сутність та специфічні особливості інформаційного протиборства та інформаційно-психологічних операцій в міжнародних відносинах.

СК16. Здатність аналізувати основи та особливості захисту національного інформаційного простору та забезпечення інформаційної

безпеки держави.

СК17. Здатність виявляти та аналізувати природу та специфічні особливості інформаційного тероризму.

У результаті вивчення навчальної дисципліни здобувачі знатимуть основні поняття, методи, підходи та тенденції міжнародної інформаційної безпеки та вмітимуть визначати місце, особливості і основні тенденції трансформації безпеки в сучасній світовій політиці у зв'язку із загальною інформатизацією і формуванням інформаційного суспільства, правильно тлумачити та застосувати міжнародні нормативно-правові акти, що необхідно для їх майбутньої трудової діяльності як фахівців у сфері міжнародної інформаційної безпеки.

1.3. Кількість кредитів – 4.

1.4. Загальна кількість годин – 120.

1.5. Характеристика навчальної дисципліни	
обов’язкова	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2-й	-
Семестр	
3-й	-
Лекції	
18 год.	-
Практичні заняття	
10 год.	-
Лабораторні заняття	
-	-
Самостійна робота	
92 год. (в т. ч. інд. завд.)	-
Індивідуальне завдання	
15 год. (контрольна робота)	-

1.6. **Заплановані програмні результати навчання:**

РН2. Знати та розуміти сутність та специфічні особливості інформаційного протиборства та інформаційно-психологічних операцій в міжнародних відносинах.

РН3. Знати та розуміти основи та особливості захисту національного інформаційного простору та забезпечення інформаційної безпеки держави.
РН4. Знати та розуміти природу та специфічні особливості інформаційного тероризму.

РН7. 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.

РН9. Визначати, оцінювати та прогнозувати політичні, дипломатичні, безпекові, суспільні й інші ризики у сфері міжнародних відносин та глобального розвитку.

РН10. Оцінювати та аналізувати міжнародні та зовнішньополітичні проблеми та ситуації, пропонувати підходи до вирішення таких проблем.

РН16. Аналізувати та оцінювати сучасні стратегії забезпечення міжнародної інформаційної безпеки.

РН17. Аналізувати та оцінювати зміст та специфіку основних напрямів діяльності міжнародних організацій в сфері безпеки.

2. ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Концепція інформаційного протиборства в міжнародних відносинах

- інформаційний чинник конфліктів у сучасних міжнародних відносинах;
- поняття та зміст інформаційного протиборства;
- форми ведення інформаційного протиборства (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 європейських держав

- Конвенція Ради Європи про кіберзлочинність 2001 року;
- Рішення Ради Міністрів ОБСЄ № 7/06 «Протидія використанню Інтернету в терористичних цілях» 2006 року;
- діяльність ЄС у сфері забезпечення інформаційної безпеки регіону;
- ініціатива «Електронна Європа» (eEurope);
- діяльність Агентства ЄС з мереж і інформаційної безпеки (ENISA);
- навчання Cyber Europe;
- діяльність Команди реагування на надзвичайні ситуації CERT-EU;
- стратегія ЄС з кібербезпеки 2013 року;
- діяльність Європейського центру по боротьбі з кіберзлочинністю (ЕС3);

- Директива 2016/1148 про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС 2016 року (NIS Directive).

Тема 5. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки американських держав і держав Азії та Азіатсько-Тихоокеанського регіону

- інструменти забезпечення інформаційної безпеки в рамках Організації Американських держав;
- роль Міжамериканської комісії з питань зв'язку (CITEL) у забезпеченні інформаційної безпеки.
- інструменти забезпечення інформаційної безпеки в рамках організації Азіатсько-Тихоокеанського економічного співробітництва (АТЕС);
- результати самітів міністрів АТЕС у сфері телекомунікацій та інформації;
- інструменти забезпечення інформаційної безпеки в рамках Асоціації держав Південно-Східної Азії;
- Регіональний форум АСЕАН з питань безпеки;
- інструменти забезпечення інформаційної безпеки в рамках Шанхайської організації співробітництва (ШОС).

3. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви змістових модулів і тем	Обсяг у годинах				Обсяг у годинах			
	Денна форма				Заочна форма			
	усього	у тому числі			усього	у тому числі		
		л	пз	с. р.		л	пз	с.р
Тема 1. Концепція інформаційного протиборства в міжнародних відносинах	22	4	2	16	-	-	-	-
Тема 2. Теоретичні засади інформаційної безпеки	17	4	2	11	-	-	-	-
Тема 3. Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру	20	2	2	16	-	-	-	-
Тема 4. Інструменти регіонального співробітництва у сфері міжнародної	20	4	2	14	-	-	-	-

інформаційної безпеки європейських держав								
Тема 5. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки американських держав і держав Азії та Азіатсько-Тихоокеанського регіону	26	4	2	20	-	-	-	-
Індивідуальне завдання	15	-	-	15	-	-	-	-
Усього годин	**120**	**18**	**10**	**92**	-	-	-	-

4. ТЕМИ ПРАКТИЧНИХ ЗАНЯТЬ

Назва теми	Кількість годин
	Денна
Тема 1. Концепція інформаційного протиборства в міжнародних відносинах	2
Тема 2. Теоретичні засади інформаційної безпеки	2
Тема 3. Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру	2
Тема 4. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки європейських держав	2
Тема 5. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки американських держав і держав Азії та Азіатсько-Тихоокеанського регіону	2
Разом	**10**

5. ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

Види, зміст самостійної роботи	Денна форма
Тема 1. Концепція інформаційного протиборства в міжнародних відносинах *Завдання*: 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Міжнародна інформаційна безпека» https://moodle.karazin.ua/course/view.php?id=3879, Тема 1) підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на практичному занятті (3 год).	16

2. Підготувати презентації доповідей з наступних тем (на вибір) та підготуватися до їх захисту на практичному занятті: - «Інформаційні війни в сучасних міжнародних відносинах»; - «Відмінність інформаційної війни від традиційної»; - «Методи інформаційно-психологічного впливу у сучасних міжнародних конфліктах» (3 год.). 3. Підготувати логіко-структурну схему на тему: «Поняття та зміст інформаційного протиборства» (2 год.). 4. Ознайомитися та проаналізувати наукову статтю: Сабрі К. Н. Інформаційно-іміджевий аспект гібридної війни. *Молодий вчений.* 2018. № 5 (57). С. 206–210. URL: http://molodyvcheny.in.ua/files/journal/2018/5/51.pdf та підготуватися до навчальної дискусії (3 год.). 5. Підготувати есе на тему та підготуватися до їх захисту: «Інструменти інформаційного протиборства сторін в російсько-українському конфлікті» та підготуватися до їх захисту (5 год.).	
Тема 2. Теоретичні засади інформаційної безпеки *Завдання*: 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Міжнародна інформаційна безпека» https://moodle.karazin.ua/course/view.php?id=3879, Тема 2) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на практичному занятті (3 год). 2. Підготувати презентації доповідей з наступних тем (на вибір) та підготуватися до їх захисту на практичному занятті (3 год.): - «Класифікації інформаційної зброї»; - «Інформаційна злочинність у сучасному світі»; 3. Підготувати есе з наступних тем (на вибір) та підготуватися до їх захисту (5 год.): - «Співвідношення понять «інформаційна безпека» та «кібербезпека»; - «Співвідношення понять «інформаційна безпека» та «міжнародна інформаційна безпека».	11
Тема 3. Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру *Завдання*: 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Міжнародна інформаційна безпека» https://moodle.karazin.ua/course/view.php?id=3879, Тема 3) та підготуватися до тестування, усного опитування та навчальної	16

дискусії за навчальними питаннями на практичному занятті (4 год). 2. Підготувати презентації доповідей з наступних тем (на вибір) та підготуватися до їх захисту на практичному занятті (4 год.): - «Операції Інтерполу проти кіберзлочинності»; - «Роль Міжнародного Союзу Електрозв'язку у забезпеченні міжнародної інформаційної безпеки». 3. Підготувати логіко-структурну схему на тему: «Резолюції ГА ООН «Досягнення у сфері інформатизації та телекомунікацій в контексті міжнародної безпеки» (3 год.). 4. Підготувати есе на тему: «Криза сучасної системи безпеки: у пошуках нового міжнародного порядку» та підготуватися до їх захисту (5 год.).	
Тема 4. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки європейських держав *Завдання:* 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Міжнародна інформаційна безпека» https://moodle.karazin.ua/course/view.php?id=3879, Тема 4) та підготуватися до тестування, усного опитування та навчальної дискусії за навчальними питаннями на практичному занятті (4 год). 2. Підготувати презентації доповідей з двох наступних тем (на вибір) та підготуватися до їх захисту на практичному занятті (6 год.): - «Роль Європолу у сфері забезпечення інформаційної безпеки регіону»; - «Діяльність Команди реагування на надзвичайні ситуації CERT-EU»; - «Діяльність Агентства ЄС з мереж і інформаційної безпеки (ENISA)»; - «Діяльність Європейського центру по боротьбі з кіберзлочинністю (ЕС3)»; - «Роль НАТО у сфері забезпечення міжнародної інформаційної безпеки». 3. Ознайомитися та проаналізувати Закон про кібербезпеку ЄС (Регламент 2019/881) https://eur-lex.europa.eu/eli/reg/2019/881/oj та скласти план-конспект основних його положень, підготуватися до навчальної дискусії (4 год.).	14

Тема 5. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки американських держав і держав Азії та Азіатсько-Тихоокеанського регіону *Завдання:* 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Міжнародна інформаційна безпека» https://moodle.karazin.ua/course/view.php?id=3879, Тема 5) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на практичному занятті та до колоквіуму за всіма темами навчальної дисципліни (5 год). 2. Підготувати презентації доповідей з наступних тем (на вибір) та підготуватися до їх захисту на практичному занятті (4 год.): - «Регіональний форум АСЕАН з питань безпеки»; - «Стратегічний план дій Робочої групи з питань телекомунікацій та інформації на 2021–2025 роки (SAP 2021–2025)»; - «Роль Міжамериканської комісії з питань зв'язку (CITEL) у забезпеченні інформаційної безпеки». 3. Підготувати схему на тему: «Результати Самітів міністрів АТЕС у сфері телекомунікацій та інформації за 1996–2021 роки» (3 год.). 4. Ознайомитися та проаналізувати Стратегію розвитку ШОС до 2025 року від 10.11.2017 року http://infoshos.ru/ru/?id=137 та скласти план-конспект основних її положень, підготуватися до навчальної дискусії (4 год.) 3. Поділитися на дві групи та підготувати питання здобувачам іншої групи за всіма темами курсу для колоквіуму на практичному занятті (4 год.).	20
Разом	**77**

6. ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

Передбачено проведення письмової контрольної роботи з метою перевірки та оцінювання набутих здобувачами знань, умінь та навичок, набутих під час вивчення дисципліни. Письмова контрольна робота передбачає собою самостійну розробку здобувачами одного питання в межах тем навчальної дисципліни. Здобувачі можуть обирати питання для розроблення в межах контрольної роботи самостійно не зі списку рекомендованих, проте обов'язково попередньо узгодивши його з викладачем.

При розкритті теоретичного питання важливо необхідно повно, глибоко і чітко висвітлити зміст обраного питання, ґрунтуючись на відповідних міжнародно-правових актах та інших джерелах. Здобувач має показати вміння використовувати і критично оцінювати теоретичні положення, що містяться у

досліджуваній літературі, аналізувати та узагальнювати матеріали, робити відповідні аргументовані висновки. Відповідь може включати схеми і таблиці, якщо вони допомагають розкрити основний зміст питання.

Структура контрольної роботи має включати: титульний лист, зміст, вступ, основний зміст, висновки, список використаних джерел, а також в разі необхідності – додатки. Обсяг контрольної роботи 20 – 25 аркушів друкованого тексту формату А4 (210х297 мм) з використанням текстового редактора Word: шрифт - Times New Roman, розмір шрифту – 14 pt; 1,5 міжрядковий інтервал; абзацний відступ – 1,25; поля: ліве – 25 мм, праве –10 мм, верхнє – 20 мм, нижнє – 20 мм.

Особливу увагу варто приділити оформленню списку використаних джерел, які мають бути подані за алфавітом, пронумеровані, оформлені відповідно до встановлених стандартів бібліографічного опису, а саме ДСТУ 8302:2015 «Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання».

При виконанні індивідуального завдання здобувачі мають дотримуватися норм академічної доброчесності.

Якщо письмова контрольна робота виконана у повному обсязі, тобто заявлена тема відповідає змісту контрольної роботи; матеріал структурований; з тексту роботи вбачається творчий підхід здобувача до розробки питання; за результатами дослідження зроблені самостійні висновки, які відповідають меті та завданням дослідження; у роботі використано не менше дванадцяти джерел, в тому числі новітні наукові публікації та не менше чотирьох іноземних; робота вчасно подана на перевірку; у ній враховані проблемні аспекти розглядуваного питання, то вона може бути оцінена до 15 балів.

Орієнтовна тематика контрольної роботи:

1. Сучасні міжнародні конфлікти.
2. Інформаційне протиборство: історичні аспекти.
3. Інформаційні війни у сучасному світі.
4. Сучасні інформаційні загрози.
5. Інформаційний тероризм як загроза міжнародній інформаційній безпеці.
6. Інформаційна злочинність як загроза міжнародній інформаційній безпеці.
7. Інформаційна зброя – зброя нового століття.
8. Проблеми забезпечення інформаційної безпеки людина в умовах ведення гібридної війни проти України.
9. Інформаційна безпека людини в міжнародному праві.
10. Роль мережі CERT у забезпеченні міжнародної інформаційної безпеки.
11. Інструменти забезпечення інформаційної безпеки в рамках організації АТЕС.
12. Інструменти забезпечення інформаційної безпеки країн Африки.
13. Операції Інтерполу проти кіберзлочинності.

14. Методи інформаційно-психологічного впливу у сучасних міжнародних конфліктах.

15. Діяльність ЄС у сфері забезпечення інформаційної безпеки регіону

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 «Міжнародна інформаційна безпека»

Шифр РН (відповідно до ОПП)	Результати навчання (відповідно до ОПП)	Методи навчання	Засоби діагностики / форми оцінювання
РН2	*Знати та розуміти сутність та специфічні особливості інформаційного протиборства та інформаційно-психологічних операцій в міжнародних відносинах.*	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями практичного заняття та за науковою статтею); виконання та захист презентації доповіді; складання логіко-структурної схеми; виконання та захист творчого завдання (есе); аналіз наукової статті; групова робота з підготовки питань до колоквіуму; колоквіум; письмова контрольна робота.	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного заняття та за результатами аналізу наукової статті); оцінювання захисту презентації доповіді та творчого завдання (есе); оцінювання виконання логіко-структурної схеми; оцінювання питань та відповідей здобувачів на колоквіумі; оцінювання письмової контрольної роботи.
РН3	*Знати та розуміти основи та особливості захисту національного інформаційного простору та забезпечення інформаційної безпеки держави.*	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями практичного заняття та за науковою статтею); виконання та захист презентації доповіді; виконання та захист творчого завдання (есе); аналіз наукової статті; групова робота з підготовки питань до	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного заняття та за результатами аналізу наукової статті); оцінювання захисту презентації доповіді та творчого завдання (есе); оцінювання питань та відповідей здобувачів на колоквіумі;

		колоквіуму; колоквіум; письмова контрольна робота.	оцінювання письмової контрольної роботи; тестування.
РН4	*Знати та розуміти природу та специфічні особливості інформаційного тероризму.*	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями практичного заняття); виконання та захист презентації доповіді; складання логіко-структурної схеми; виконання та захист творчого завдання (есе); аналіз наукової статті; групова робота з підготовки питань до колоквіуму; колоквіум; письмова контрольна робота.	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного заняття); оцінювання захисту презентації доповіді та творчого завдання (есе);оцінювання виконання логіко-структурної схеми; оцінювання питань та відповідей здобувачів на колоквіумі; оцінювання письмової контрольної роботи.
РН7	*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.*	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями практичного заняття та за науковою статтею, міжнародними правовими актами); виконання та захист презентації доповіді; складання логіко-структурної схеми; виконання та захист творчого завдання (есе); аналіз наукової статті; групова робота з підготовки питань до колоквіуму; колоквіум; письмова контрольна робота.	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного заняття та за результатами аналізу наукової статті, міжнародних правових актів); оцінювання захисту презентації доповіді та творчого завдання (есе);оцінювання виконання логіко-структурної схеми; оцінювання питань та відповідей здобувачів на колоквіумі; оцінювання письмової контрольної роботи; тестування.
РН9	*Визначати, оцінювати та прогнозувати політичні, дипломатичні, безпекові, суспільні й інші ризики у сфері міжнародних відносин та глобального*	Лекція-дискусія; усне опитування; навчальна дискусія (за питаннями практичного заняття та за науковою статтею, міжнародними	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного заняття та за результатами аналізу наукової

	розвитку.	правовими актами); виконання та захист презентації доповіді; складання логіко-структурної схеми; виконання та захист творчого завдання (есе); аналіз наукової статті; групова робота з підготовки питань до колоквіуму; колоквіум; письмова контрольна робота.	статті, міжнародних правових актів); оцінювання захисту презентації доповіді та творчого завдання (есе);оцінювання виконання логіко-структурної схеми; оцінювання питань та відповідей здобувачів на колоквіумі; оцінювання письмової контрольної роботи; тестування.
РН10	*Оцінювати та аналізувати міжнародні та зовнішньополітичні проблеми та ситуації, пропонувати підходи до вирішення таких проблем.*	Лекція-дискусія; усне опитування; навчальна дискусія (за питаннями практичного заняття та за науковою статтею, міжнародними правовими актами); виконання та захист презентації доповіді; складання логіко-структурної схеми; виконання та захист творчого завдання (есе); аналіз наукової статті; групова робота з підготовки питань до колоквіуму; колоквіум; письмова контрольна робота.	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного заняття та за результатами аналізу наукової статті, міжнародних правових актів); оцінювання захисту презентації доповіді та творчого завдання (есе);оцінювання виконання логіко-структурної схеми; оцінювання питань та відповідей здобувачів на колоквіумі; оцінювання письмової контрольної роботи; тестування.
РН16.	*Аналізувати та оцінювати сучасні стратегії забезпечення міжнародної інформаційної безпеки.*	Лекція-дискусія; усне опитування; навчальна дискусія (за питаннями практичного заняття та міжнародними правовими актами); виконання та захист презентації доповіді; складання логіко-структурної схеми; виконання та захист творчого завдання (есе); аналіз наукової статті; групова робота з підготовки	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного заняття та за результатами аналізу міжнародних правових актів); оцінювання захисту презентації доповіді та творчого завдання (есе);оцінювання виконання логіко-структурної схеми; оцінювання питань та

		питань до колоквіуму; колоквіум; письмова контрольна робота.	відповідей здобувачів на колоквіумі; оцінювання письмової контрольної роботи; тестування.
РН17	*Аналізувати та оцінювати зміст та специфіку основних напрямів діяльності міжнародних організацій в сфері безпеки.*	Лекція-дискусія; усне опитування; навчальна дискусія (за питаннями практичного заняття та міжнародними правовими актами); виконання та захист презентації доповіді; складання логіко-структурної схеми; виконання та захист творчого завдання (есе); аналіз наукової статті; групова робота з підготовки питань до колоквіуму; колоквіум; письмова контрольна робота.	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного заняття та міжнародних правових актів); оцінювання захисту презентації доповіді та творчого завдання (есе);оцінювання виконання логіко-структурної схеми; оцінювання питань та відповідей здобувачів на колоквіумі; оцінювання письмової контрольної роботи; тестування.

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

– проходження тренінг-курсів чи дистанційних курсів з використання сучасних освітніх технологій на платформах Coursera, Prometheus тощо (за наявності відповідного документу про їх закінчення, надання копії викладачу);

– участь в майстер-класах, форумах, конференціях, семінарах, зустрічах з проблем використання сучасних освітніх технологій (з підготовкою есе, прес-релізу, інформаційного повідомлення тощо, що підтверджено навчальною програмою заходу чи відповідним сертифікатом);

– участь у науково-дослідних та прикладних дослідженнях з проблем використання сучасних освітніх технологій (в розробці анкетних форм, проведенні опитувань, підготовці та проведенні фокус-груп, обробці результатів дослідження, підготовці звіту, презентації результатів тощо, що підтверджується демонстрацією відповідних матеріалів).

8. МЕТОДИ КОНТРОЛЮ.

Засвоєння тем розділів (поточний контроль) здійснюється на практичних заняттях відповідно до контрольних цілей. Основне завдання поточного контролю – перевірка рівня підготовки здобувачів до виконання конкретної роботи.

Поточний контроль і оцінювання результатів навчання передбачає виставлення оцінок за всіма формами проведення занять:

- контроль та оцінювання активності роботи здобувача під час лекційних та практичних занять (усне опитування, навчальна дискусія за питаннями практичного заняття);
- контроль та оцінювання якості підготовки та розробки проєктних завдань в ході індивідуальної / групової роботи здобувачів (підготовка питань до колоквіуму);
- контроль засвоєння теоретичного та практичного матеріалу (у вигляді тестування, колоквіуму);
- контроль та оцінювання вмінь вирішувати аналітичні та інші завдання (навчальна дискусія за результатами аналізу наукових статей та міжнародних правових актів);
- контроль та оцінювання вмінь проводити дослідження та презентувати із застосуванням сучасних інформаційних технологій (захист презентацій доповідей; захист есе);
- оцінювання вмінь та навичок складати схеми, збирати, систематизувати та оброблювати дані (підготовка логіко-структурних схем).

При вивченні кожної теми проводиться поточний контроль. На практичному занятті здобувач може отримати від 7 до 12 балів. Максимально здобувач може отримати 45 балів в ході лекційних та практичних занять.

Перевірка виконання **індивідуального завдання** (письмової контрольної роботи) завданням якої є оцінювання знань, умінь та практичних навичок здобувачів, набутих під час вивчення зазначених тем, проводиться по завершенню практичних занять. Максимальна кількість балів за індивідуальне завдання (письмову контрольну роботу) становить 15 балів.

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

Підсумковий контроль засвоєння тем навчальної дисципліни в здійснюється по їх завершенню шляхом проведення екзамену. Завданням контролю є оцінювання знань, умінь та практичних навичок здобувачів, набутих під час вивчення зазначених тем. Вміст екзаменаційного білета й оцінювання відповідей на екзамені: 40 тестових питань закритого типу з однією правильною відповіддю; максимальна кількість балів – 40 (правильна відповідь на одне тестове питання оцінюється в 1 бал).

Таблиця 8.1

Критерії та методи оцінювання

Методи	Критерії оцінювання	Система оцінювання, бали
Усне опитування / навчальна дискусія за питаннями практичного заняття	Висока активність здобувача на практичному занятті, демонстрація засвоєння повного обсягу матеріалу теми, ознайомлення із запропонованими джерелами, уміння робити висновки	2
	Активність здобувача на практичному занятті, демонстрація засвоєння повного обсягу матеріалу теми, ознайомлення із запропонованими джерелами, уміння робити висновки, але здобувач припустився окремих помилок.	1
Тестування за питаннями практичного заняття	За кожною темою, де передбачено тестування, пропонується 10 тестових питань закритого типу з однією правильною відповіддю. Правильна відповідь на 1 питання оцінюється в 0,1 бала.	0,1–1
Навчальна дискусія за результатами аналізу науковою статтею / міжнародними правовими актами	Висока активність здобувача на практичному занятті, демонстрація ознайомлення із запропонованим матеріалом, уміння мислити аналітично, формувати та виражати своє ставлення до предмета дискусії, робити висновки.	2
	Активність здобувача на практичному занятті, демонстрація ознайомлення із запропонованим матеріалом, уміння мислити аналітично, формувати та виражати своє ставлення до предмета дискусії, робити висновки, але здобувач припустився окремих помилок.	1
Підготовка та захист презентацій доповідей	Змістовна відповідність презентації доповіді запропонованій темі та її повне розкриття, формальна відповідність методичним рекомендація до підготовки презентацій доповідей, що розміщено в дистанційному курсі «Міжнародна інформаційна безпека» https://moodle.karazin.ua/course/view.php?id=3879 , демонстрація засвоєння знань програмного матеріалу та умінь їх застосовувати на практиці при виконанні та захисті презентації доповіді, вміння робити висновки, обґрунтовувати власну позицію.	2
	Змістовна відповідність презентації доповіді запропонованій темі та її розкриття, окремі вади формальної відповідності методичним рекомендаціям до підготовки презентацій доповідей, що розміщено в дистанційному курсі «Міжнародна інформаційна безпека» https://moodle.karazin.ua/course/view.php?id=3879 , демонстрація засвоєння знань програмного матеріалу та умінь їх застосовувати на практиці при виконанні та захисті презентації доповіді, вміння робити висновки.	1
Перевірка складання логіко-	Відповідність схеми запропонованій темі, повнота використання матеріалу за темою схеми, наявність логіко-структурних зв’язків між елементами схеми, демонстрація	1

структурної схеми	засвоєння знань програмного матеріалу та умінь їх застосовувати.	
Виконання та захист творчого завдання (есе)	Змістовна відповідність есе обраній темі та її повне розкриття, формальна відповідність методичним рекомендація до підготовки есе, що розміщено в дистанційному курсі «Міжнародна інформаційна безпека» https://moodle.karazin.ua/course/view.php?id=3879 , демонстрація систематизованих та глибоких знань програмного матеріалу та умінь їх застосовувати на практиці при виконанні та захисті есе, вміння грамотно інтерпретувати одержані результати на рівні творчого використання, вміння робити висновки, демонстрація ознайомлення із запропонованими джерелами.	3
	Змістовна відповідність есе обраній темі та її розкриття, окремі несуттєві вади формальної відповідності методичним рекомендація до підготовки есе, що розміщено в дистанційному курсі «Міжнародна інформаційна безпека» https://moodle.karazin.ua/course/view.php?id=3879 , демонстрація систематизованих знань програмного матеріалу та умінь їх застосовувати на практиці при виконанні та захисті есе, вміння грамотно інтерпретувати одержані результати на рівні творчого використання, вміння робити висновки, демонстрація ознайомлення із окремими запропонованими джерелами.	2
	Змістовна відповідність есе обраній темі та її неповне розкриття, окремі суттєві вади формальної відповідності методичним рекомендація до підготовки есе, що розміщено в дистанційному курсі «Міжнародна інформаційна безпека» https://moodle.karazin.ua/course/view.php?id=3879 , демонстрація знань програмного матеріалу та умінь їх застосовувати на практиці при виконанні та захисті есе, вміння інтерпретувати одержані результати на рівні творчого використання, вміння робити висновки, демонстрація ознайомлення із окремими запропонованими джерелами.	1
Перевірка групової роботи з підготовки питань до колоквіуму	Демонстрація систематизованих та глибоких знань програмного матеріалу та умінь їх застосовувати на практиці при підготовці питань для колоквіуму, демонстрація ознайомлення та роботи із запропонованими джерелами, творчий підхід до підготовки питань.	2
	Демонстрація базових знань програмного матеріалу та умінь їх застосовувати на практиці при підготовці питань для колоквіуму, демонстрація ознайомлення та роботи з окремими запропонованими джерелами.	1
Колоквіум	Висока активність здобувача на практичному занятті, демонстрація засвоєння повного обсягу матеріалу теми, ознайомлення із запропонованими джерелами, уміння робити висновки.	3
	Активність здобувача на практичному занятті, демонстрація засвоєння повного обсягу матеріалу теми, ознайомлення із більшістю запропонованих джерел, уміння робити висновки, але здобувач припустився окремих	2

	несуттєвих помилок.	
	Активність здобувача на практичному занятті, демонстрація засвоєння матеріалу навчальної дисципліни , ознайомлення із окремими запропонованими джерелами, уміння робити висновки, але здобувач припустився окремих суттєвих помилок.	1
Індивідуальне завдання (письмова контрольна робота)	Обрана тема контрольної роботи повністю відповідає її змісту; тема є оригінальною; матеріал якісно структурований; здобувачем використано творчий підхід до вирішення суті поставленого проблемного питання, висновки зроблені здобувачем самостійно; робота вчасно здана викладачеві; здобувачем використано не менше дванадцяти літературних джерел, використані новітні наукові публікації, в тому числі іноземні (не менше чотирьох), список використаних джерел оформлений правильно відповідно до вимог ДСТУ 8302:2015.	14–15
	Обрана тема контрольної роботи повністю відповідає її змісту; матеріал якісно структурований; здобувачем використано творчий підхід до вирішення суті поставленого проблемного питання, висновки зроблені здобувачем самостійно; здобувачем використано не менше десяти літературних джерел, в тому числі іноземні (не менше трьох), але не використані новітні наукові публікації; є помилки при оформленні списку використаних джерел, робота здана із запізненням.	10–13
	Обрана тема контрольної роботи не в повному обсязі відповідає її змісту; матеріал структурований, але є неточності; здобувачем використано не менше восьми літературних джерел , але не використані новітні наукові публікації та/або іноземні, або використано менше двох іноземних джерел; здобувач не використовував творчий підхід до вирішення суті поставленого проблемного питання; відсутні самостійні висновки за результатами виконання контрольної роботи; робота здана викладачеві із значним запізненням; мають місце значні помилки при оформленні списку використаних джерел.	5–9
	Обрана тема контрольної роботи частково відповідає її змісту; здобувачем використано не менше п’яти літературних джерел, але не використані новітні наукові публікації та іноземні публікації; здобувач не використовував творчий підхід до вирішення суті поставленого проблемного питання; відсутні самостійні висновки за результатами виконання контрольної роботи; матеріал неякісно структурований; робота здана викладачеві із запізненням; список використаних джерел оформлений із значними помилками.	1–4
	Обрана тема контрольної роботи повністю не відповідає її змісту; матеріал неякісно структурований або взагалі неструктурований; здобувач не використовував творчий підхід до вирішення суті поставленого проблемного питання; відсутні самостійні висновки за результатами виконання контрольної роботи; робота здана викладачеві	0

	із запізненням або не здана; здобувачем використано менше п’яти літературних джерел, не використані новітні наукові публікації та іноземні публікації; список використаних джерел оформлений із значними помилками або відсутній; мають місце порушення академічної доброчесності.	
Підсумковий контроль (тестування)	Здобувач правильно відповів на всі тестові питання.	40
	Здобувач правильно відповів на не менш, ніж 75 % тестових питань.	30–39
	Здобувач правильно відповів на не менш, ніж 50 % тестових питань.	20–29
	Здобувач правильно відповів на не менш ніж 25 % тестових питань.	10–19
	Здобувач правильно відповів на менш, ніж 25 % тестових питань.	1–9
	Здобувач не відповів на жодне з тестових питань.	0

9. СХЕМА НАРАХУВАННЯ БАЛІВ

Поточне оцінювання роботи здобувачів на практичних заняттях та самостійної роботи					Індивідуальне завдання (письмова контрольна робота, передбачена навчальним планом)	Всього	Екзамен	Сума
Т1	Т2	Т3	Т4	Т5		60	40	100
10	7	9	7	12	15			

Відповідно, максимальна кількість набраних балів по вивченню дисципліни складає 100 балів.

Оцінювання здійснюється відповідно до шкали ЗВО.

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. Гапаєва О. Міжнародна інформаційна безпека – ключовий напрям діяльності Шанхайської організації співробітництва: 2006–2017 рр. *Східноєвропейський історичний вісник.* 2017. Вип. 4. С. 155–163.
3. Дереко В.Н. Теоретико-методологічні засади класифікації загроз об'єктам інформаційної безпеки. *Інформаційна безпека людини, суспільства, держави.* 2015. № 2 (18). С.16–22.
4. Доценко О. М. Дистанційний курс «Міжнародна інформаційна безпека». URL: https://moodle.karazin.ua/course/view.php?id=3879
5. Лапінська Є. І. Інформаційна безпека: поняття, види та ознаки. *Порівняльно-аналітичне право.* 2018. № 6. С. 262–266.
6. Макаренко Є. А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст. *Актуальні проблеми міжнародних відносин.* 2011. Випуск 102 (Частина І). С. 160–164.
7. Макаренко Є. Інформаційне протиборство 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).
8. 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.
9. 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).
10. Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2nd ed. Syngress, 2014. 240 p.

Допоміжна література

11. 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.visnykjuris.uzhnu.uz.ua/file/No.31/part_3/33.pdf (дата звернення: 20.08.2021).
12. Інформаційна безпека (соціально-правові аспекти) / В. Остроухов, В. Петрик, М. Присяжнюк та ін. ; за ред. Є.Д. Скулиша. К. : КНТ, 2010. 776 с.
13. Карпов О. Н. Можливості використання баз даних Міжнародної організації кримінальної поліції – Інтерпол у протидії тероризму. *Питання інформаційної безпеки.* 2009. № 21. С. 301–306.

14. Король А. Інформаційні технології в системі міжнародних відносин: проблема впровадження. *Мультиверсум. Філософський альманах.* 2015. Випуск 3–4 (141–142). С. 59–67.

15. 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: 20.08.2021).

16. 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.

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

18. 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: 20.08.2021).

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

20. 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/VndWdmIxY WFBQUVNaTc4Y25aWkxISVpLSXRPQjBiK0lHakYrMlNIa3JOZGhkaWRNUnR ZbTVBPT0=/attachment/VFEyQTQ4M3ptUWNCZ0ErcVdweUc2Mnlzc0hRQ2gwV Wg= (Last Accessed: 20.08.2021).

11. ПОСИЛАННЯ НА ІНФОРМАЦІЙНІ РЕСУРСИ В ІНТЕРНЕТІ, ВІДЕО-ЛЕКЦІЇ, ІНШЕ МЕТОДИЧНЕ ЗАБЕЗПЕЧЕННЯ

1. About APEC. Asia-Pacific Economic Cooperation : веб-сайт. URL: https://www.apec.org/About-Us/About-APEC (Last Accessed: 20.08.2021).
2. About CSIRTs Network. CIRTsNEtwork : web-site. URL: https://csirtsnetwork.eu/ (Last Accessed: 20.08.2021).
3. About ENISA. ENISA : web-site. URL: https://www.enisa.europa.eu/about-enisa (Last Accessed: 20.08.2021).
4. About Us. CERT-EU. URL: https://cert.europa.eu/cert/plainedition/en/cert_about.html (Last Accessed: 20.08.2021).
5. Cyber Europe 2020. URL: https://www.enisa.europa.eu/topics/cyberexercises/cybereurope-programme/cyber-europe-2020/ (Last Accessed: 20.08.2021).
6. European Cybercrime Centre - EC3. Combating crime in a digital age. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (Last Accessed: 20.08.2021).

7. The Shanghai Cooperation Organisation. The Shanghai Cooperation Organisation : вебсайт. URL: http://eng.sectsco.org/about_sco/ (Last Accessed: 20.08.2021).

8. Who we are. OAS : веб-сайт. URL: http://www.oas.org/en/about/who_we_are.asp (Last Accessed: 20.08.2021).

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 (https://us06web.zoom.us/j/92063081526?pwd=UGZubFRUMEVQUW9EZk83dHc5bnorQT09 , ідентифікатор конференції: 920 6308 1526, код доступа: AjJ8Gz);

– аудиторно (за затвердженим розкладом занять) проводяться до 10% практичних занять у навчальних групах кількістю до 20 осіб з урахуванням відповідних санітарних і протиепідемічних заходів.