Додаток 5

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
Олександр ГОЛОВКО

"31" 03 2022
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»

спеціалізація

вид дисципліни обов'язкова

факультет міжнародних економічних відносин та туристичного бізнесу

2022/ 2023 навчальний рік

Програму рекомендовано до затвердження вченою радою факультету міжнародних економічних відносин та туристичного бізнесу "30" серпня 2022 року, протокол №1

РОЗРОБНИКИ ПРОГРАМИ: канд. юрид. наук, доцент кафедри міжнародних відносин, міжнародної інформації та безпеки Олена Доценко

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

Протокол від "26" серпня 2022 року № 1

Завідувач кафедри міжнародних відносин, міжнародної інформації та безпеки

Людмила НОВІКОВА

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

Гарант освітньо-професійної програми «Міжнародна інформаційна безпека»

Людмила НОВІКОВА

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

Протокол від "29" серпня 2022 року № 1

Голова науково-методичної комісії факультету
міжнародних економічних відносин та туристичного бізнесу

Лариса ГРИГОРОВА-БЕРЕНДА

ВСТУП

Програма навчальної дисципліни «Міжнародна інформаційна безпека» складена відповідно до освітньо-професійної програми підготовки «Міжнародна інформаційна безпека» другого (магістерського) рівня вищої освіти спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни: 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 вирішення складних спеціалізованих задач та практичних проблем під час їх майбутньої професійної діяльності у сфері міжнародних відносин, зовнішньої політики, міжнародних комунікацій що характеризуються комплексністю та невизначеністю умов, передбачають проведення досліджень та/або запровадження інновацій з фаховим акцентом на міжнародну інформаційну безпеку.

1.2. Основні завдання вивчення дисципліни:

- формування наступних загальних компетентностей:

ЗК 2. Здатність вчитися і оволодівати сучасними знаннями.

ЗК 3. Вміння виявляти, ставити та вирішувати проблеми.

ЗК 6. Здатність працювати в міжнародному контексті.

- формування наступних фахових компетентностей:

СК 2. Здатність приймати обґрунтовані рішення щодо здійснення міжнародної та зовнішньополітичної діяльності.

СК 3. Здатність аргументувати вибір шляхів вирішення завдань професійного характеру у сфері міжнародних відносин, суспільних комунікацій та регіональних студій, критично оцінювати отримані результати та обґрунтовувати прийняті рішення.

СК 5. Здатність аналізувати та прогнозувати міжнародні відносини у різних контекстах, зокрема політичному, безпековому, правовому, економічному, суспільному, культурному та інформаційному.

СК 7. Здатність здійснювати прикладні аналітичні дослідження проблем міжнародних відносин та світової політики, суспільних комунікацій, регіональних студій, професійно готувати аналітичні матеріали та довідки.

СК 9. Здатність виявляти та аналізувати особливості розвитку країн та регіонів, сучасних глобальних, регіональних та локальних процесів, та місця в них України.

СК 11. Здатність аналізувати природу та джерела зовнішньої політики, еволюцію підходів до її формування та здійснення, принципи організації системи зовнішньої політики та функціонування інститутів зовнішньої політики.

СК 14. Здатність оцінювати зміст та основні напрями діяльності міжнародних організацій в сфері безпеки та сучасних стратегій забезпечення міжнародної інформаційної безпеки.

СК 15. Здатність виявляти та аналізувати сутність та специфічні особливості інформаційного протиборства та інформаційно-психологічних операцій в міжнародних відносинах.

СК 16. Здатність аналізувати основи та особливості захисту національного інформаційного простору та забезпечення інформаційної безпеки держави.

СК 17. Здатність виявляти та аналізувати природу та специфічні особливості інформаційного тероризму.

1.3. Кількість кредитів: 6

1.4. Загальна кількість годин: 180

1.5. Характеристика навчальної дисципліни	
обов'язкова	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
1-й	-
Семестр	
2-й	-
Лекції	
32 год.	-
Семінарські заняття	
16 год.	-
Лабораторні заняття	
- год.	-
Самостійна робота	
132 год. (в т. ч. індивідуальне завдання)	-
у тому числі індивідуальні завдання (курсова робота)	
- год.	-

1.6. Заплановані результати навчання:

РН 1. Знати та розуміти природу, джерела та напрями еволюції міжнародних відносин, міжнародної політики, зовнішньої політики держав, стан теоретичних досліджень міжнародних відносин та світової політики.

РН 2. Знати та розуміти сутність та специфічні особливості інформаційного протиборства та інформаційно-психологічних операцій в міжнародних відносинах.

РН 3. Знати та розуміти основи та особливості захисту національного інформаційного простору та забезпечення інформаційної безпеки держави.

РН 4. Знати та розуміти природу та специфічні особливості інформаційного тероризму.

РН 6. Застосовувати сучасні наукові підходи, методології та методики для дослідження проблем міжнародних відносин та зовнішньої політики.

РН 7. 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.

РН 9. Визначати, оцінювати та прогнозувати політичні, дипломатичні, безпекові, суспільні й інші ризики у сфері міжнародних відносин та глобального розвитку.

РН 10. Оцінювати та аналізувати міжнародні та зовнішньополітичні проблеми та ситуації, пропонувати підходи до вирішення таких проблем.

РН 16. Аналізувати та оцінювати сучасні стратегії забезпечення міжнародної інформаційної безпеки.

РН 17. Аналізувати та оцінювати зміст та специфіку основних напрямів діяльності міжнародних організацій в сфері безпеки.

РН 19. Брати участь у професійній дискусії у сфері міжнародних відносин, зовнішньої політики, суспільних комунікацій та регіональних студій, поважати опонентів і їхню точку зору, доносити до фахівців та широкого загалу інформацію, ідеї, проблеми, рішення та власний досвід з фахових проблем.

РН 20. Організовувати та вести професійні дискусії у сфері міжнародних відносин, зовнішньої політики, суспільних комунікацій та регіональних студій.

РН 22. Демонструвати здатність до подальшого навчання з високим рівнем автономності.

2. Тематичний план навчальної дисципліни

Розділ 1. Загальні засади міжнародної інформаційної безпеки

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.

Розділ 2. Окремі аспекти 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 (EC3);
- Директива 2016/1148 про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС 2016 року (NIS Directive).

Тема 5. Інструменти НАТО у сфері міжнародної інформаційної безпеки

- стандарти НАТО у сфері міжнародної інформаційної безпеки;
- політика НАТО у сфері інформаційної безпеки;
- співробітництво Україна–ЄС–НАТО з протидії гібридним загрозам.

Тема 6. 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).

Тема 7. Цифрова дипломатія в контексті міжнародної інформаційної безпеки

- поняття дипломатії та її місце в зовнішньополітичній діяльностідержави;
- генеза та зміст поняття «цифрова дипломатія»;
- інструменти цифрової дипломатії;
- веб-сайти зовнішньополітичних відомств та дипломатичнихпредставництв як інструмент цифрової дипломатії;
- соціальні мережі як інструмент цифрової дипломатії;
- досвід цифрової дипломатії держав Європи та України.

Тема 8. Міжнародно-правове регулювання транскордонного управління Інтернетом

- історичні та теоретико-правові засади становлення та розвитку міжнародно-правового регулювання транскордонного управління Інтернетом;
- багатостороння модель транскордонного управління Інтернетом;
- транскордонне управління Інтернетом на універсальному рівні;
- транскордонне управління Інтернетом на регіональному рівні.

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п/с	лаб	інд.	с.р.		л	п/с	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Загальні засади захисту міжнародної інформаційної безпеки												
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	17	4	2	-	-	11	-	-	-	-	-	-
Разом за розділом 1	**56**	**12**	**6**	**-**	**-**	**38**	**-**	**-**	**-**	**-**	**-**	**-**
Розділ 2. Окремі аспекти міжнародної інформаційної безпеки												
Тема 4. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки європейських держав	16	4	2	-	-	10	-	-	-	-	-	-

Тема 5. Інструменти НАТО у сфері міжнародної інформаційної безпеки	22	3	2	-	-	17	-	-	-	-	-	-
Тема 6. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки американських держав і держав Азії та Азіатсько-Тихоокеанського регіону	15	3	2			10						
Тема 7. Цифрова дипломатія в контексті міжнародної інформаційної безпеки	18	5	2	-	-	11	-	-	-	-	-	-
Тема 8. Міжнародно-правове регулювання транскордонного управління Інтернетом	18	5	2	-	-	11	-	-	-	-	-	-
Разом за розділом 2	**89**	**20**	**10**	**-**	**-**	**59**	**-**	**-**	**-**	**-**	**-**	**-**
Індивідуальне завдання (Курсова робота)	**35**	**-**	**-**	**-**	**-**	**35**						
Усього годин	**180**	**32**	**16**	**-**	**-**	**132**	**-**	**-**	**-**	**-**	**-**	**-**

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	Тема 1. Концепція інформаційного протиборства в міжнародних відносинах	2
2	Тема 2. Теоретичні засади інформаційної безпеки	2
3	Тема 3. Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру	2
4	Тема 4. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки європейських держав	2
5	Тема 5. Інструменти НАТО у сфері міжнародної інформаційної безпеки	2
6	Тема 6. Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки американських держав і держав Азії та Азіатсько-Тихоокеанського регіону	2
7	Тема 7. Цифрова дипломатія в контексті міжнародної інформаційної безпеки	2
8	Тема 8. Міжнародно-правове регулювання транскордонного управління Інтернетом	2
	Разом	**16**

5. Завдання для самостійної роботи

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	**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=5237 , Тема 1) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (5 год). 2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на семінарському занятті: 1) «Інформаційні війни в сучасних міжнародних відносинах»; 2) «Відмінність інформаційної війни від традиційної»; 3) «Методи інформаційно-психологічного впливу у сучасних міжнародних конфліктах» (5 год.). 3. Підготувати аналітичний огляд на тему: «Інструменти інформаційного протиборства сторін в російсько-українському конфлікті», представити у вигляді таблиці (6 год.).	16
2	**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=5237 , Тема 2) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті, а також до розв'язання тестових завдань (6 год). 2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на семінарському занятті: 1) «Класифікації інформаційної зброї»; 2) «Інформаційна злочинність у сучасному світі» (5 год.).	11
3	**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=5237 , Тема 3) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (5 год). 2. Підготувати есе на тему «Криза сучасної системи безпеки: у пошуках нового міжнародного порядку» та підготуватися до його захисту (6 год.).	11
4	**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=5237 , Тема 4) та	10

	підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (5 год). 2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на семінарському занятті: 1) «Роль Європолу у сфері забезпечення інформаційної безпеки регіону»; 2) «Діяльність Команди реагування на надзвичайні ситуації CERT-EU»; 3) «Діяльність Агентства ЄС з мереж і інформаційної безпеки (ENISA)»; 4) «Діяльність Європейського центру по боротьбі з кіберзлочинністю (ЕС3)» (5 год.).	
5	**Тема 5. Інструменти НАТО у сфері міжнародної 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=5237 , Тема 5) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (5 год). 2. Підготувати аналітичний огляд на тему: «Сучасний стан забезпечення інформаційної та кібербезпеки в країнах НАТО (на прикладах реагування на інциденти)» (країни НАТО обрати самостійно) (6 год.). 3. Підготувати есе на тему «Перспективи набуття Україною членства у НАТО у сучасних умовах: значення для протидії загрозам в інформаційній сфері» та підготуватися до його захисту (6 год.).	17
6	**Тема 6. 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=5237 , Тема 6) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (5 год). 2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на семінарському занятті: 1) «Регіональний форум АСЕАН з питань безпеки»; 2) «Стратегічний план дій Робочої групи з питань телекомунікацій та інформації на 2021–2025 роки (SAP 2021–2025)»; 3) «Роль Міжамериканської комісії з питань зв'язку (CITEL) у забезпеченні інформаційної безпеки»; 4) «Результати Самітів міністрів АТЕС у сфері телекомунікацій та інформації за 1996–2022 роки» (5 год.).	10
7	**Тема 7. Цифрова дипломатія в контексті міжнародної 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=5237 , Тема 7) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (5 год). 2. Підготувати дослідницький проєкт на тему: «Цифрова дипломатія	11

	певної країни світу» (країну обрати самостійно) та підготуватися до його захисту на семінарському занятті (6 год.).	
8	**Тема 8. Міжнародно-правове регулювання транскордонного управління Інтернетом** *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=5237 , Тема 8) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті, а також до розв'язання тестових завдань (6 год). 2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на семінарському занятті: 1) EuroDIG (Європейський форум з управління Інтернетом); 2) Український форум з управління Інтернетом; 3) Всесвітній форум з управління Інтернетом (20-22 роки) (5 год.).	11
	Разом	**97**

6. Індивідуальні завдання

Передбачено проведення курсової роботи з метою перевірки та оцінювання набутих здобувачами знань, умінь та навичок, набутих під час вивчення навчальної дисципліни. Курсова робота передбачає собою самостійну розробку здобувачами однієї теми в межах тематики навчальної дисципліни. Здобувачі можуть обирати тему для розроблення в межах курсової роботи самостійно не зі списку рекомендованих, проте обов'язково попередньо узгодивши його з викладачем.

При розкритті теми 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 курсової роботи має включати: титульний лист, зміст, вступ, основний зміст, висновки, список використаних джерел, а також в разі необхідності – додатки. Обсяг курсової роботи 30 – 35 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 курсова робота виконана у повному обсязі, тобто заявлена тема відповідає змісту курсової 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 двадцяти джерел, в тому числі новітні наукові публікації та не менше шести іноземних; список використаних джерел оформлений правильно відповідно до вимог ДСТУ 8302:2015; робота вчасно подана на перевірку; у ній враховані проблемні аспекти розглядуваного питання, то вона може бути оцінена максимально у 20 балів.

Орієнтовна тематика курсових робіт:

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 «Захист національного інформаційного простору»

Шифр РН (відповідно до ОПП)	Результати навчання (відповідно до ОПП)	Методи навчання	Засоби діагностики / форми оцінювання
РН 1	Знати та розуміти природу, джерела та напрями еволюції міжнародних відносин, міжнародної політики, зовнішньої політики держав, стан теоретичних досліджень міжнародних відносин та світової політики.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд; есе; курсова робота.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.
РН 2	Знати та розуміти сутність та специфічні особливості інформаційного протиборства та інформаційно-психологічних	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд; есе; курсова робота.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду;

	операцій в міжнародних відносинах.		оцінювання есе; тестування; оцінювання курсової роботи.
РН 3	Знати та розуміти основи та особливості захисту національного інформаційного простору та забезпечення інформаційної безпеки держави.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд; есе; курсова робота.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.
РН 4	Знати та розуміти природу та специфічні особливості інформаційного тероризму.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд; есе; курсова робота.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.
РН 6	Застосовувати сучасні наукові підходи, методології та методики для дослідження проблем міжнародних відносин та зовнішньої політики.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд; есе.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.
РН 7	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 семінарського заняття); дослідницький проєкт; аналітичний огляд; есе; курсова робота.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.
РН 9	Визначати, оцінювати та прогнозувати політичні,	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття);	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського

	дипломатичні, безпекові, суспільні й інші ризики у сфері міжнародних відносин та глобального розвитку.	дослідницький проєкт; аналітичний огляд; есе; курсова робота.	заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.
РН 10	Оцінювати та аналізувати міжнародні та зовнішньополітичні проблеми та ситуації, пропонувати підходи до вирішення таких проблем.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд; есе; курсова робота.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.
РН 16	Аналізувати та оцінювати сучасні стратегії забезпечення міжнародної інформаційної безпеки.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд; есе; курсова робота.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.
РН 17	Аналізувати та оцінювати зміст та специфіку основних напрямів діяльності міжнародних організацій в сфері безпеки.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд; есе; курсова робота.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.
РН 19	Брати участь у професійній дискусії у сфері міжнародних відносин, зовнішньої політики, суспільних комунікацій та регіональних студій, поважати опонентів і їхню точку зору, доносити до фахівців та широкого загалу інформацію, ідеї, проблеми, рішення	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд; есе; курсова робота.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.

	та власний досвід з фахових проблем.		
РН 20	Організовувати та вести професійні дискусії у сфері міжнародних відносин, зовнішньої політики, суспільних комунікацій та регіональних студій.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд; есе; курсова робота.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.
РН 22	Демонструвати здатність до подальшого навчання з високим рівнем автономності.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд; есе; курсова робота.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання есе; тестування; оцінювання курсової роботи.

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 фундаментальних та прикладних наукових 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 (поточний контроль) здійснюється на семінарських 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 семінарських занять (усне опитування, навчальна дискусія за питаннями заняття);
- контроль та оцінювання якості підготовки та розробки проєктних завдань в ході індивідуальної / групової роботи здобувачів (виконання та захист дослідницьких проєктів);
- контроль засвоєння теоретичного та практичного матеріалу (тестування; усне опитування за питаннями семінарського заняття);
- контроль та оцінювання вмінь вирішувати аналітичні та інші завдання (здійснення аналітичних оглядів);
- контроль та оцінювання вмінь проводити дослідження та презентувати із

застосуванням сучасних інформаційних технологій (виконання та захист дослідницьких проєктів, есе);

- оцінювання вмінь та навичок складати схеми, збирати, систематизувати та оброблювати дані (здійснення аналітичних оглядів).

При вивченні кожної теми проводиться поточний контроль. На семінарському занятті здобувач може отримати від 4 до 7 балів. Загальна сума балів за виконання завдань для самостійної роботи та роботу на семінарських заняттях може сягати 40 балів.

Перевірка виконання **індивідуального завдання** (курсової роботи) завданням якої є оцінювання знань, умінь та практичних навичок здобувачів, набутих під час вивчення зазначених тем, проводиться по завершенню семінарських занять. Максимальна кількість балів за індивідуальне завдання (курсову роботу) становить 20 балів. Загальна сума балів за виконання завдань для самостійної роботи, роботу на семінарських 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).

9. Схема нарахування балів

Поточний контроль та самостійна робота								Індивідуальне завдання	Разом	Екзамен	Сума
Розділ 1				Розділ 2							
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	20	60	40	100
6	5	5	5	7	4	4	4				

Т1, Т2 ... – теми розділів.

Таблиця 8.1

Критерії та методи оцінювання навчальних досягнень

Методи	Критерії оцінювання	Система оцінювання, бали
Усне опитування, навчальна дискусія за питаннями семінарського заняття	Висока активність здобувача на семінарському занятті, демонстрація засвоєння повного обсягу матеріалу теми, ознайомлення із запропонованими джерелами, уміння робити висновки.	**1,6–2**
	Середня здобувача на семінарському занятті, демонстрація засвоєння неповного обсягу матеріалу теми, ознайомлення із запропонованими джерелами, уміння робити висновки, але здобувач припустився окремих помилок.	**1,–1,5**
	Незначна активність здобувача на семінарському занятті, демонстрація засвоєння окремих аспектів матеріалу теми, ознайомлення з частиною запропонованих джерел, уміння робити висновки, але здобувач припустився значних помилок.	**0,5–1**

	Неактивність активність здобувача на семінарському занятті, демонстрація незасвоєння матеріалу теми, неознайомлення чи ознайомлення з незначною частиною запропонованих джерел, неуміння робити висновки.	**0-0,4**
Аналітичний огляд	Змістовна відповідність та повнота аналітичного огляду запропонованій темі; наявність логіко-структурних зв'язків між елементами огляду; демонстрація ознайомлення із всіма запропонованими матеріалами; інформацію подано у вигляді систематизованих стислих висновків-тез.	**1,8–2**
	Змістовна відповідність та повнота аналітичного огляду запропонованій темі; наявність логіко-структурних зв'язків між елементами огляду з незначними помилками; демонстрація ознайомлення з більшістю запропонованих матеріалів; інформацію подано у вигляді систематизованих висновків з незначними помилками.	**1,5–1,7**
	Змістовна відповідність та недостатня повнота аналітичного огляду запропонованій темі; наявність логіко-структурних зв'язків між елементами огляду із значними помилками; демонстрація ознайомлення з частиною запропонованих матеріалів; інформацію подано у вигляді висновків, але з помилками.	**1,1–1,4**
	Неповна змістовна відповідність та недостатня повнота аналітичного огляду запропонованій темі; наявність логіко-структурних зв'язків між елементами огляду із значними помилками; демонстрація ознайомлення з частиною запропонованих матеріалів; інформацію подано у вигляді висновків, але із значними помилками.	**0,7–1**
	Часткова змістовна відповідність та неповнота аналітичного огляду запропонованій темі; відсутність або наявність логіко-структурних зв'язків між елементами огляду із значними помилками; демонстрація ознайомлення із незначною частиною запропонованих матеріалів; інформацію подано у вигляді висновків, але із значними помилками.	**0,4–0,7**
	Незначна змістовна відповідність або невідповідність аналітичного огляду запропонованій темі; відсутність логіко-структурних зв'язків між елементами огляду; демонстрація ознайомлення із незначною частиною запропонованих матеріалів або неознайомлення із матеріалами; інформацію подано хаотично, не у вигляді висновків, або не подано.	**0-0,3**
Дослідницький проєкт	Змістовна відповідність дослідницького проєкту запропонованій темі та її повне розкриття; формальна відповідність методичним рекомендаціям; демонстрація повного засвоєння знань програмного матеріалу та умінь його застосовувати на практиці при виконанні та захисті дослідницького проєкту; демонстрація вмінь аналізувати та робити висновки, обґрунтовувати власну позицію.	**1,7–2**

	Змістовна відповідність дослідницького проєкту запропонованій темі та її достатньо повне розкриття; формальна відповідність методичним рекомендаціям з незначними помилками; демонстрація часткового засвоєння знань програмного матеріалу та умінь його застосовувати на практиці при виконанні та захисті дослідницького проєкту; демонстрація вмінь аналізувати та робити висновки з незначними помилками, обґрунтовувати власну позицію.	**1,3–1,6**
	Часткова змістовна відповідність дослідницького проєкту запропонованій темі та її часткове розкриття; формальна відповідність методичним рекомендаціям із значними помилками або невідповідність; демонстрація часткового засвоєння знань програмного матеріалу та умінь його застосовувати на практиці при виконанні та захисті дослідницького проєкту із суттєвими помилками; часткова демонстрація вмінь аналізувати та робити висновки із суттєвими помилками, обґрунтовувати власну позицію.	**0,8–1,2**
	Часткова змістовна відповідність дослідницького проєкту запропонованій темі та її часткове розкриття; формальна відповідність методичним рекомендаціям із значними помилками або невідповідність; демонстрація вибіркового засвоєння знань програмного матеріалу та часткових умінь його застосовувати на практиці при виконанні та захисті дослідницького проєкту із суттєвими помилками; допущення суттєвих помилок у вміннях аналізувати та робити висновки, обґрунтовувати власну позицію або невміння аналізувати та робити висновки, обґрунтовувати власну позицію.	**0,4–0,7**
	Часткова змістовна відповідність дослідницького проєкту запропонованій темі та її часткове розкриття; формальна відповідність методичним рекомендаціям із значними помилками або невідповідність; демонстрація вибіркового засвоєння знань програмного матеріалу та часткових умінь його застосовувати на практиці при виконанні та захисті дослідницького проєкту із суттєвими помилками; допущення суттєвих помилок у вміннях аналізувати та робити висновки, обґрунтовувати власну позицію або невміння аналізувати та робити висновки, обґрунтовувати власну позицію.	**0-0,3**
Виконання та захист творчого завдання (есе)	Змістовна відповідність есе обраній темі та її повне розкриття, формальна відповідність методичним рекомендаціям; 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	**2,5–3**
	Змістовна відповідність есе обраній темі та її розкриття, окремі несуттєві вади формальної відповідності методичним рекомендаціям; демонстрація систематизованих знань програмного матеріалу та умінь	**1,5–2,4**

	їх застосовувати на практиці при виконанні та захисті есе, вміння грамотно інтерпретувати одержані результати на рівні творчого використання, вміння робити висновки, але з помилками, демонстрація ознайомлення із окремими запропонованими джерелами.	
	Змістовна відповідність есе обраній темі та її неповне розкриття, окремі суттєві вади формальної відповідності методичним рекомендаціям; 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.	**0,6–1,4**
	Змістовна невідповідність есе обраній темі або її неповне розкриття, формальна невідповідність методичним рекомендаціям; демонстрація знань програмного матеріалу та умінь їх застосовувати на практиці при виконанні та захисті есе з суттєвими помилками; невміння інтерпретувати одержані результати на рівні творчого використання, невміння робити висновки, демонстрація ознайомлення із окремими запропонованими джерелами або неознайомлення з ними.	**0-0,5**
Тестування	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**
Індивідуальне завдання (курсова робота)	Курсова робота виконана у повному обсязі, тобто заявлена тема відповідає змісту курсової 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 двадцяти джерел, в тому числі новітні наукові публікації та не менше шести іноземних; список використаних джерел оформлений правильно відповідно до вимог ДСТУ 8302:2015 або з незначними неточностями; робота вчасно подана на перевірку; у ній враховані проблемні аспекти розглядуваного питання.	**18–20**
	Курсова робота виконана у повному обсязі, тобто заявлена тема відповідає змісту курсової роботи; матеріал структурований, але мають місце структурно-логічні неточності; 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 менше двадцяти джерел та/або не використано новітні наукові публікації та менше шести іноземних; список використаних джерел оформлений відповідно до вимог ДСТУ 8302:2015, але з незначними помилками; робота вчасно подана на перевірку; у ній	**13–17**

	враховані проблемні аспекти розглядуваного питання.	
	Курсова робота виконана не в повному обсязі, тобто заявлена тема відповідає змісту курсової роботи частково; матеріал не структурований або структурований із структурно-логічними помилками; з тексту роботи вбачається творчий підхід здобувача до розробки питання; за результатами дослідження зроблені самостійні висновки, які частково відповідають меті та завданням дослідження; у роботі використано менше дванадцяти джерел та/або не використано новітні наукові публікації та менше трьох іноземних; список використаних джерел оформлений відповідно до вимог ДСТУ 8302:2015, але з суттєвими помилками; робота вчасно подана на перевірку; у ній враховано більшість проблемних аспектів розглядуваного питання.	**8–12**
	Курсова робота виконана не в повному обсязі, тобто заявлена тема відповідає змісту курсової роботи частково; матеріал не структурований або структурований із суттєвими структурно-логічними помилками; з тексту роботи не вбачається творчий підхід здобувача до розробки питання; за результатами дослідження зроблені самостійні висновки, які частково відповідають меті та завданням дослідження; у роботі використано менше десяти джерел та/або не використано новітні наукові публікації та менше двох іноземних або не використано іноземні джерела; список використаних джерел оформлений відповідно до вимог ДСТУ 8302:2015, але з суттєвими помилками; робота невчасно подана на перевірку; у ній частково враховано проблемні аспекти розглядуваного питання.	**4–7**
	Курсова робота виконана не в повному обсязі, тобто заявлена тема відповідає змісту курсової роботи частково або не відповідає; матеріал не структурований або структурований із суттєвими структурно-логічними помилками; з тексту роботи не вбачається творчий підхід здобувача до розробки питання; висновки за результатами дослідження зроблені несамостійно або не відповідають меті та завданням дослідження; у роботі використано менше п’яти джерел та/або не використано новітні наукові публікації та не використано іноземні джерела; список використаних джерел оформлений відповідно до вимог ДСТУ 8302:2015 з суттєвими помилками або не у відповідності з ДСТУ 8302:2015; робота невчасно подана на перевірку; у ній не враховано проблемні аспекти розглядуваного питання; у роботі мають місце порушення академічної доброчесності	**0–3**
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**

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. Алексєєва Т. І. Міжнародні організації: сучасні пріоритети та нові виклики в системі міжнародної інформаційної безпеки. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство.* 2020. Випуск 34. С. 9–12. URL: http://www.visnyk-econom.uzhnu.uz.ua/archive/34_2020ua/3.pdf (дата звернення: 20.08.2022).
2. 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
3. Гапаєва О. Міжнародна інформаційна безпека – ключовий напрям діяльності Шанхайської організації співробітництва: 2006–2017 рр. *Східноєвропейський історичний вісник.* 2017. Вип. 4. С. 155–163.
4. 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: 20.08.2022).
5. Кононенко В. П., Новікова Л. В., Копицька П. О. Політика міжнародних організацій з питань інформаційної безпеки. *Науковий вісник Ужгородського національного університету. Серія: ПРАВО.* 2021. Випуск 65. С. 353–358. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/242834/240747 (дата звернення: 20.08.2022).
6. Копійка М .В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. *Політичне життя.* 2020. № 1. С. 102–109.
7. Лапінська Є. І. Інформаційна безпека: поняття, види та ознаки. Порівняльноаналітичне право. 2018. № 6. С. 262–266.
8. 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: 20.08.2022)
9. 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: 20.08.2022).
10. 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.

11. Младьонова О. Д. Інформаційна безпека як складова національної безпеки України. *Вісник ХНУ імені В. Н. Каразіна. Серія «Питання політології».* 2017. Вип. 31. С. 87–92. URL: https://periodicals.karazin.ua/politology/article/view/9596 (дата звернення: 03.05.2022).

12. Ткачук Т. Інформаційна безпека держави в національному законодавстві європейських країн. Visegrad Journal on Human Rights. 2018. № 1 (Volume 2). С. 145–150. URL: http://vjhr.sk/archive/2018_1/part_2/24.pdf (дата звернення: 20.08.2022).

13. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. Підприємництво, господарство і право. 2017. № 10. С. 182–186. URL: http://pgpjournal.kiev.ua/archive/2017/10/38.pdf (дата звернення: 20.08.2022).

14. 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).

15. Dickinson S. China's New Cybersecurity System: There is NO Place to Hide. October 7, 2019. Harris Bricken : web-site. URL: https://www.chinalawblog.com/2019/10/chinas-new-cybersecurity-system-there-is-no-place-tohide.html (Last Accessed: 20.08.2022).

16. Şeker E., Tolga I. B. National Cyber Security Organisation: Turkey. Tallinn, 2018. 20 p.

17. The Privacy, Data Protection and Cybersecurity Law Review / ed. Raul A. Ch. Sixth edition. United Kingdom, Law Business Research Ltd, 2019. 442 p. URL: https://thelawreviews.co.uk//digital_assets/a3cf7f19-36b0-4627-84fe-805c58ab9ae7/ThePrivacy-Data-Protection-and-Cybersecurity-Law-Review-Edition-6-secured.pdf (Last Accessed: 20.08.2022).

18. Vozniuk E., Ukrainka L. Principles and Features of Japan's Information Security System. *Політичне життя.* 2017. № 4. С. 8–12.

Допоміжна 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. Валюшко 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.

3. Ничипорук Н., Вознюк Є. Секрет успіху США у сфері інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії. 2018.* № 1 (3). С. 66–71.

4. Пазюк А. В. Міжнародно-правове регулювання інформаційної сфери (теоретичні і практичні аспекти) : дис. … док. юрид. Наук: 12.00.11 / Київський національний університет імені Тараса Шевченка. Київ, 2016. 467 с. URL: https://www.academia.edu/22357125/%D0%9C%D0%86%D0%96%D0%9D%D0%90%D0%A0%D0%9E%D0%94%D0%9D%D0%9E_%D0%9F%D0%A0%D0%90%D0%92%D0%9E%D0%92%D0%95_%D0%A0%D0%95%D0%93%D0%A3%D0%9B%D0%AE%D0%92%D0%90%D0%9D%D0%9D%D0%AF_%D0%86%D0%9D%D0%A4%D0%9E%D0%A0%D0%9C%D0%90%D0%A6%D0%86%D0%99%D0%9D%D0%9E%D0%87_%D0%A1%D0%A4%D0%95%D0%A0%D0%98_%D0%A2%D0%95%D0%9E%D0%A0%D0%95%D0%A2%D0%98%D0%A7%D0%9D%D0%86_%D0%86_%D0%9F%D0%A0%D0%90%D0%9A%D0%A2%D0%98%D0%A7%D0%9D%D0%86_%D0%90%D0%A1%D0%9F%D0%95%D0%9A%D0%A2%D0%98_ (дата звернення: 20.08.2022).

5. Семен Н. Ф. Російські Інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «Правда.Ру» та «Российский диалог»): дис. … канд. наук з соц. комун.: 27.00.01 / Міжнародний економіко-гуманітарний університет імені акад. С. Демянчука; Дніпровський національний університет імені Олеся Гончара. Рівне, 2018. 250 с.

6. 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.

7. Horenbeeck M. V. Cybersecurity Culture, Norms and Values. Background paper to the IGF Best Practices Forum on Cybersecurity. IGF 2018 Best Practices Forum on Cybersecurity. URL:

https://www.academia.edu/37417784/Cybersecurity_Culture_Norms_and_Values (Last Accessed: 20.08.2022).

8. Grygorov O., Basysta A., Yedeliev R., Paziuk A., Tropin Z. International cyber security strategy as a tool for comprehensive security assurance of civil aviation security: methodological considerations. *IJCSNS International Journal of Computer Science and Network Security*. 2021. VOL. 21. No. 9. P. 332–338. URL: https://www.academia.edu/61040486/International_Cyber_Security_Strategy_as_a_Tool_for_Comprehensive_Security_Assurance_of_Civil_Aviation_Security_Methodological_Considerations (Last Accessed: 20.08.2022).

9. Paziuk A., Mitsik v. Global cybersecurity culture in the international discourse: values ans principles. *Вісник Національної академії керівних кадрів культури і мистецтв.*2019. № 2. С. 103–107. URL: https://www.academia.edu/52573669/Global_Cybersecurity_Culture_in_the_International_Discourse_Values_and_Principles (дата звернення: 20.08.2022).

10. Molander R. C., Riddile A. S., Wilson P. A. Strategic Information Warfare: A New Face of War. RAND Corporation. URL: https://www.rand.org/pubs/monograph_reports/MR661/index2.html (Last Accessed: 20.08.2022).

11. 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
16. About APEC. Asia-Pacific Economic Cooperation : веб-сайт. URL: https://www.apec.org/About-Us/About-APEC
17. About CSIRTs Network. CIRTsNEtwork : web-site. URL: https://csirtsnetwork.eu/
18. About ENISA. ENISA : web-site. URL: https://www.enisa.europa.eu/about-enisa
19. About Us. CERT-EU. URL: https://cert.europa.eu/cert/plainedition/en/cert_about.html
20. Cyber Europe 2020. URL: https://www.enisa.europa.eu/topics/cyberexercises/cybereurope-programme/cyber-europe-2020/
21. European Cybercrime Centre - EC3. Combating crime in a digital age. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
22. The Shanghai Cooperation Organisation. The Shanghai Cooperation Organisation : вебсайт. URL: http://eng.sectsco.org/about_sco/
23. Who we are. OAS : веб-сайт. URL: http://www.oas.org/en/about/who_we_are.asp
24. Computer Emergency Response Team of Ukraine (CERT-UA) – https://cert.gov.ua/

25. Офіційний сайт кіберполіції України – https://cyberpolice.gov.ua/

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

В умовах дії карантинних обмежень або запровадження військового стану освітній процес в університеті здійснюється за дистанційною формою навчання, а саме: дистанційно (за затвердженим розкладом занять) на платформі Zoom (https://us05web.zoom.us/j/4115712639?pwd=YWpJQ3VCSmQwRFdMRFZrakVwaWZCdz09, ідентифікатор конференції: 411 571 2639, код доступа: 620976) проводяться всі лекційні та семінарські заняття, а також завдання для роботи на семінарських заняттях та самостійної роботи виконуються на платформі moodle (https://moodle.karazin.ua/course/view.php?id=5237)

Додаток 1

Додаток до робочої програми навчальної дисципліни «Міжнародна інформаційна безпека»

Дію робочої програми продовжено: на 20_____/20_____н. р.

Заступник декана_____факультету з навчальної роботи

_____ _____
(підпис) (прізвище, ініціали)

«____»_____20___р.

Голова науково-методичної комісії_____факультету

_____ _____
(підпис) (прізвище, ініціали)

«____»_____20___р.