

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 серпня 2022 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Інформаційний тероризм

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 за вибором

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 «Інформаційний тероризм» 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 поняття, видів, напрямів протидії інформаційному тероризму на національному та міжнародному рівнях, а також практичних умінь та навичок визначення загроз, що створює інформаційний тероризм в сучасних міжнародних відносинах, застосування способів та інструментів протидії інформаційному тероризму, правильного тлумачення та застосування міжнародних документів, необхідних для їх майбутньої трудової діяльності як фахівців у сфері міжнародних відносин, зовнішньої політики та міжнародних комунікацій з акцентом на міжнародну інформаційну безпеку.

1.2. Основні завдання вивчення дисципліни:

- формування наступних загальних компетентностей:

ЗК 1. Здатність проводити дослідження на відповідному рівні.

ЗК 3. Вміння виявляти, ставити та вирішувати проблеми.

ЗК 5. Здатність генерувати нові ідеї (креативність).

ЗК 8. Здатність виявляти ініціативу та підприємливість.

ЗК 10. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК 12. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

- формування наступних фахових компетентностей:

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

СК 5. Здатність аналізувати глобальні процеси та їх вплив на міжнародні та суспільні відносини, політичні та суспільні системи.

СК 6. Здатність використовувати для дослідження міжнародних відносин, суспільних комунікацій та для регіональних студій теоретичні та методологічні підходи політології, економічної та правової науки, міждисциплінарних досліджень.

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: 4

1.4. Загальна кількість годин: 120

1.5. Характеристика навчальної дисципліни	
За вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2-й	-
Семестр	
3-й	-
Лекції	
18 год.	-
Практичні, семінарські заняття	
9 год.	-
Лабораторні заняття	
- год.	-
Самостійна робота	
93 год.	-
у тому числі індивідуальні завдання	
	-

1.6. Заплановані результати навчання:

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

РН 7. Аналізувати та оцінювати проблеми міжнародної та національної безпеки, міжнародні та інтернаціоналізовані конфлікти, підходи, способи та механізми забезпечення безпеки у міжнародному просторі 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.

2. Тематичний план навчальної дисципліни

Розділ 1. Інформаційний тероризм як загроза національній та міжнародній інформаційній безпеці

Тема 1. Тероризм як загроза безпеці в сучасних міжнародних відносинах

- виникнення та розвиток тероризму в міжнародних відносинах;
- наукові підходи до визначення поняття «тероризм»;
- форми прояву та види тероризму в сучасних міжнародних відносинах;
- інструменти протидії тероризму на універсальному рівні;
- інструменти протидії тероризму на регіональному рівні (на прикладі європейського регіону);
- інструменти протидії тероризму на національному рівні: досвід для України.

Тема 2. Поняття та види інформаційного тероризму

- поняття «інформаційний тероризм» та його характерні риси;
- прояви, форми, способи вчинення інформаційного тероризму;
- види інформаційного тероризму;
- медіа-тероризм, його характерні риси та способи здійснення;
- кібертероризм, його характерні риси, види та способи здійснення.

Розділ 2. Протидія інформаційному тероризму на універсальному, регіональному та національному рівнях

Тема 3. Інструменти протидії інформаційному тероризму на універсальному рівні

- протидія інформаційному тероризму в рамках ООН;
- роль Інтерполу у протидії інформаційному тероризму;

Тема 4. Інструменти протидії інформаційному тероризму на регіональному рівні

- протидія інформаційному тероризму в рамках Ради Європи;
- протидія інформаційному тероризму в рамках ЄС;
- протидія інформаційному тероризму в рамках НАТО;
- протидія інформаційному тероризму в рамках ОБСЄ;
- протидія інформаційному тероризму в рамках ОАД;
- протидія інформаційному тероризму в рамках ШОС;
- протидія інформаційному тероризму в рамках АСЕАН;
- протидія інформаційному тероризму в рамках АТЕС;
- протидія інформаційному тероризму в рамках Африканського Союзу.

Тема 5. Інформаційний тероризм як загроза національній безпеці України

- нормативно-правові інструменти протидії інформаційному тероризму в Україні;
- інституційні інструменти протидії інформаційному тероризму в Україні;
- співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму.

Тема 6. Інструменти протидії інформаційному тероризму зарубіжних країн

- особливості протидії інформаційному тероризму в США та інших країнах американського континенту;
- особливості протидії інформаційному тероризму в країнах Європи;
- особливості протидії інформаційному тероризму в країнах Азії.
- особливості протидії інформаційному тероризму в країнах Африки та Австралії.

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	лаб.	інд.	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Інформаційний тероризм як загроза національній та міжнародній інформаційній безпеці												
Тема 1. Тероризм як загроза безпеці в сучасних міжнародних відносинах	22	4	1	-	-	17	-	-	-	-	-	-
Тема 2. Поняття та види інформаційного тероризму	17	4	2	-	-	11	-	-	-	-	-	--

Разом за розділом 1	39	8	3	-	-	28	-	-	-	-	-	-
Розділ 2. Протидія інформаційному тероризму на універсальному, регіональному та національному рівнях												
Тема 3. Інструменти протидії інформаційному тероризму на універсальному рівні	13	1	1	-	-	11	-	-	-	-	-	-
Тема 4. Інструменти протидії інформаційному тероризму на регіональному рівні	28	3	2	-	-	23	-	-	-	-	-	-
Тема 5. Інформаційний тероризм як загроза національній безпеці України	17	2	1	-	-	14	-	-	-	-	-	-
Тема 6. Інструменти протидії інформаційному тероризму зарубіжних країн	23	4	2	-	-	17	-	-	-	-	-	-
Разом за розділом 2	81	10	6	-	-	65	-	-	-	-	-	-
Усього годин	120	18	9	-	-	93	-	-	-	-	-	-

4. Темі семінарських та практичних занять

№ з/п	Назва теми	Кількість годин
1	Тема 1. Тероризм як загроза безпеці в сучасних міжнародних відносинах	1
2	Тема 2. Поняття та види інформаційного тероризму	2
3	Тема 3. Інструменти протидії інформаційному тероризму на універсальному рівні	1
4	Тема 4. Інструменти протидії інформаційному тероризму на регіональному рівні	2
5	Тема 5. Інформаційний тероризм як загроза національній безпеці України	1
6	Тема 6. Інструменти протидії інформаційному тероризму зарубіжних країн	2
	Разом	9

5. Завдання для самостійної роботи

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	Тема 1. Тероризм як загроза безпеці в сучасних міжнародних відносинах Завдання: 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Інформаційний тероризм» https://moodle.karazin.ua/course/view.php?id=5794 , Тема 1) та	17

	<p>підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на практичному/семінарському занятті (5 год).</p> <p>2. Підготувати аналітичний огляд резолюцій ООН щодо протидії тероризму, представити у вигляді таблиці (6 год.).</p> <p>3. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на практичному/семінарському занятті:</p> <p>1) «Найгучніші терористичні акти ХХІ століття: загальна характеристика»; 2) «Інструменти протидії тероризму на регіональному рівні» (азійський чи американський регіон на вибір).</p> <p>3) «Інструменти протидії тероризму в Україні» (6 год.).</p>	
2	<p>Тема 2. Поняття та види інформаційного тероризму</p> <p><i>Завдання:</i></p> <p>1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Інформаційний тероризм» https://moodle.karazin.ua/course/view.php?id=5794, Тема 2) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на практичному/семінарському занятті, а також до розв'язання тестових завдань (6 год).</p> <p>2. Ознайомитися з науковими статтями https://www.usip.org/sites/default/files/sr119.pdf та https://www.tandfonline.com/doi/pdf/10.1080/1057610X.2021.1928887?needAccess=true, поділитися на 2 команди та підготувати командою анотацію на одну із запропонованих статей (5 год).</p>	11
3	<p>Тема 3. Інструменти протидії інформаційному тероризму на універсальному рівні</p> <p><i>Завдання:</i></p> <p>1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Інформаційний тероризм» https://moodle.karazin.ua/course/view.php?id=5794, Тема 3) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на практичному/семінарському занятті (4 год).</p> <p>2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на практичному/семінарському занятті:</p> <p>1) «Роль Управління ООН щодо протидії тероризму у боротьбі з інформаційним тероризмом»; 2) «Роль Контртерористичного центру ООН у боротьбі з інформаційним тероризмом»; 3) «Форуми та конференції під егідою ООН щодо протидії інформаційному тероризму»; 4) «Операції Інтерполу щодо протидії інформаційному тероризму» (7 год.)</p>	11
4	<p>Тема 4. Інструменти протидії інформаційному тероризму на регіональному рівні</p> <p><i>Завдання:</i></p> <p>1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Інформаційний тероризм» https://moodle.karazin.ua/course/view.php?id=5794, Тема 4) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на практичному/семінарському занятті (4</p>	23

	<p>год).</p> <p>2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на практичному/семінарському занятті:</p> <p>1) «Протидія інформаційному тероризму в рамках ОАД»;</p> <p>2) «Протидія інформаційному тероризму в рамках ШОС»;</p> <p>3) «Протидія інформаційному тероризму в рамках АСЕАН та АТЕС»;</p> <p>4) «Протидія інформаційному тероризму в рамках Африканського Союзу» (7 год.).</p> <p>3. Ознайомитися з науковою статтею https://www.cambridge.org/core/journals/british-journal-of-political-science/article/cyber-terrorism-and-public-support-for-retaliation-a-multicountry-survey-experiment/179C0560441076100DB4A4E5BBCB992F та підготувати анотацію (6 год).</p> <p>4. Поділитися на 2 команди та підготувати аналітичний огляд інформаційних/кібератак на країни різних регіонів (на вибір) протягом останніх 10 років, представити у вигляді таблиці (6 год.).</p>	
5	<p>Тема 5. Інформаційний тероризм як загроза національній безпеці України</p> <p><i>Завдання:</i></p> <p>1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Інформаційний тероризм» https://moodle.karazin.ua/course/view.php?id=5794, Тема 5) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на практичному/семінарському занятті, а також до розв'язання тестових завдань (5 год).</p> <p>2. Ознайомитися з документальним фільмом «Інформаційний тероризм» https://www.youtube.com/watch?v=PziD0tDuxX0 та бути готовим до навчальної дискусії та обґрунтування своєї точки зору щодо інформації, наведеної у фільмі, на практичному/семінарському занятті (3 год).</p> <p>3. Поділитися на 2 команди та підготувати аналітичний огляд інформаційних/кібератак на Україну протягом останніх 10 років, представити у вигляді таблиці (6 год.).</p>	14
6	<p>Тема 6. Інструменти протидії інформаційному тероризму зарубіжних країн</p> <p><i>Завдання:</i></p> <p>1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Інформаційний тероризм» https://moodle.karazin.ua/course/view.php?id=5794, Тема 6) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на практичному/семінарському занятті (4 год).</p> <p>2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до їх захисту на практичному/семінарському занятті: «Особливості протидії інформаційному тероризму в певній країні світу» (обрати країну на вибір) (7 год.).</p> <p>3. Ознайомитися з науковою статтею https://law.stanford.edu/wp-content/uploads/2018/03/stocktongoldman.pdf, поділитися на 2</p>	17

	команди та підготувати анотації (6 год).	
	Разом	93

6. Індивідуальні завдання

Не передбачено.

7. Методи навчання

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

Таблиця 7.1

Методи навчання та засоби діагностики результатів навчання за освітньою компонентною «Інформаційний тероризм»

Шифр РН (відповідно до ОПП)	Результати навчання (відповідно до ОПП)	Методи навчання	Засоби діагностики / форми оцінювання
РН 2	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/семінарського заняття); дослідницький проект; аналітичний огляд (командна робота); анотація на наукову статтю.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями практичного/семінарського заняття); оцінювання захисту дослідницького проекту; оцінювання аналітичного огляду, оцінювання анотації на наукову статтю.
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 практичного/семінарського заняття); навчальна дискусія за відеоматеріалами; дослідницький проект; аналітичний огляд (командна робота); анотація на наукову статтю (командна робота).	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями практичного/семінарського заняття); оцінювання виступу здобувача під час навчальної дискусії за відеоматеріалами; оцінювання захисту дослідницького проекту; оцінювання аналітичного огляду, оцінювання анотації на наукову статтю; тестування.
РН 4	Знати та розуміти природу та специфічні особливості інформаційного тероризму.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями практичного/семінарського заняття); дискусія за відеоматеріалами;	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями практичного/семінарського заняття); оцінювання

		дослідницький проєкт; аналітичний огляд (командна робота); анотація на наукову статтю (індивідуально та командна робота).	виступу здобувача під час навчальної дискусії за відеоматеріалами; оцінювання дослідницького проєкту; оцінювання аналітичного огляду; оцінювання анотації на наукову статтю; тестування.
PH 5	Критично осмислювати та аналізувати глобальні процеси та їх вплив на міжнародні відносини.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями практичного/семінарського заняття); дослідницький проєкт; аналітичний огляд міжнародних документів; аналітичний огляд (командна робота); анотація на наукову статтю.	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного/семінарського заняття); оцінювання дослідницького проєкту; оцінювання аналітичного огляду міжнародних документів; оцінювання аналітичного огляду; оцінювання анотації.
PH 7	Аналізувати та оцінювати проблеми міжнародної та національної безпеки, міжнародні та інтернаціоналізовані конфлікти, підходи, способи та механізми забезпечення безпеки у міжнародному просторі у зовнішній політиці держав.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями практичного/семінарського заняття); навчальна дискусія за відеоматеріалами; аналітичний огляд міжнародних документів; дослідницький проєкт; аналітичний огляд (командна робота); анотація на наукову статтю (індивідуально та командна робота).	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного/семінарського заняття); оцінювання виступу здобувача під час навчальної дискусії за відеоматеріалами; оцінювання дослідницького проєкту; оцінювання аналітичного огляду; оцінювання анотації на наукову статтю; тестування.
PH 9	Визначати, оцінювати та прогнозувати політичні, дипломатичні, безпекові, суспільні й інші ризики у сфері міжнародних відносин та глобального розвитку.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями практичного/семінарського заняття); дослідницький проєкт; аналітичний огляд міжнародних документів; анотація на наукову статтю (командна робота).	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного/семінарського заняття); оцінювання дослідницького проєкту; оцінювання аналітичного огляду міжнародних документів; оцінювання анотації.
PH 10	Оцінювати та аналізувати міжнародні та зовнішньополітичні проблеми та ситуації,	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями практичного/семінарського	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за

	пропонувати підходи до вирішення таких проблем.	заняття); дослідницький проєкт; аналітичний огляд міжнародних документів; аналітичний огляд (командна робота); анотація на наукову статтю (індивідуально та командна робота).	питаннями практичного/семінарського заняття); оцінювання дослідницького проєкту; цінювання аналітичного огляду; оцінювання анотації; тестування.
PH 16	Аналізувати та оцінювати сучасні стратегії забезпечення міжнародної інформаційної безпеки.	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями практичного/семінарського заняття); аналітичний огляд міжнародних документів; аналітичний огляд (командна робота); анотація на наукову статтю (індивідуально та командна робота).	Оцінювання усних відповідей здобувачів та виступів під час навчальної дискусії (за питаннями практичного/семінарського заняття); оцінювання аналітичного огляду міжнародних документів; оцінювання аналітичного огляду; оцінювання анотації; 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 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 практичних/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 практичних/семінарських занять (усне опитування, навчальна дискусія за питаннями практичного / заняття; навчальна дискусія за відеоматеріалами);

- 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 практичного/семінарського заняття);

- контроль та оцінювання вмінь вирішувати аналітичні та інші завдання (здійснення аналітичних оглядів; підготовка анотацій на наукові статті);

- контроль та оцінювання вмінь проводити дослідження та презентувати із застосуванням сучасних інформаційних технологій (виконання та захист дослідницьких проєктів);

- оцінювання вмінь та навичок складати схеми, збирати, систематизувати та оброблювати дані (здійснення аналітичних оглядів; підготовка анотацій на наукові статті).

При вивченні кожної теми проводиться поточний контроль. На практичному / семінарському занятті здобувач може отримати від 6 до 16 балів.

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

Підсумковий контроль засвоєння тем навчальної дисципліни в здійснюється по їх завершенню шляхом проведення заліку. 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						Разом	Залікова робота	Сума
Розділ 1		Розділ 2						
T1	T2	T3	T4	T5	T6	60	40	100
10	6	7	16	10	11			

T1, T2 ... – теми розділів.

Таблиця 8.1

Критерії та методи оцінювання навчальних досягнень

Методи	Критерії оцінювання	Система оцінювання, бали
Усне опитування, навчальна дискусія за питаннями практичного/ семінарського заняття	Висока активність здобувача на практичному / семінарському занятті, демонстрація засвоєння повного обсягу матеріалу теми, ознайомлення із запропонованими джерелами, уміння робити висновки.	2,5–3
	Середня здобувача на практичному / семінарському занятті, демонстрація засвоєння неповного обсягу матеріалу теми, ознайомлення із запропонованими джерелами, уміння робити висновки, але здобувач припустився окремих помилок.	1,5–2,4
	Незначна активність здобувача на практичному / семінарському занятті, демонстрація засвоєння окремих аспектів матеріалу теми, ознайомлення з частиною запропонованих джерел, уміння робити висновки, але здобувач припустився значних помилок.	0,6–1,4
	Неактивність активність здобувача на практичному / семінарському занятті, демонстрація незасвоєння матеріалу теми, незнайомення чи ознайомення з незначною частиною запропонованих джерел, неуміння робити висновки.	0-0,5
Навчальна	Висока активність здобувача на практичному /	1,5–2

дискусія за відеоматеріалами	семінарському занятті, демонстрація повного засвоєння відеоматеріалів, уміння аналізувати засвоєну інформацію та робити висновки.	
	Середня активність здобувача на практичному / семінарському занятті, демонстрація часткового засвоєння відеоматеріалів, уміння аналізувати засвоєну інформацію та робити висновки.	0,6-1,4
	Неактивність здобувача на практичному / семінарському занятті, демонстрація незасвоєння або засвоєння незначної частини відеоматеріалів, невміння аналізувати засвоєну інформацію та робити висновки.	0-0,5
Аналітичний огляд міжнародних документів	Змістовна відповідність та повнота аналітичного огляду запропонованій темі; наявність хронологічних/логіко-структурних зв'язків між елементами огляду; демонстрація ознайомлення із всіма міжнародними документами за темою; інформацію подано у вигляді систематизованих стислих висновків по кожному документу.	2,5-3
	Змістовна відповідність аналітичного огляду запропонованій темі; наявність незначних помилок у визначенні хронологічних/логіко-структурних зв'язків між елементами огляду; демонстрація ознайомлення із більшістю міжнародних документів за темою; інформацію подано у вигляді систематизованих стислих висновків по кожному документу.	1,5-2,4
	Змістовна відповідність аналітичного огляду запропонованій темі, але допущені помилки; наявність значних помилок у визначенні хронологічних/логіко-структурних зв'язків між елементами огляду; демонстрація ознайомлення з деякими міжнародними документами за темою; інформацію подано у вигляді стислих висновків по кожному документу.	0,6-1,4
	Змістовна невідповідність аналітичного огляду запропонованій темі або наявність значних змістовних помилок; наявність значних помилок у визначенні хронологічних/логіко-структурних зв'язків між елементами огляду; демонстрація ознайомлення із вибіркковими міжнародними документами за темою, або неознайомлення з ними; інформацію подано не у вигляді систематизованих стислих висновків по кожному документу, а хаотично.	0-0,5
Аналітичний огляд (командна робота)	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; наявний самостійний розподіл ролей між учасниками команди і вклад кожного у проведення аналітичного огляду; презентація аналітичного огляду відповідно до розподілених ролей.	4,5-5
	Змістовна відповідність та повнота аналітичного огляду запропонованій темі; наявність логіко-структурних зв'язків між елементами огляду з незначними помилками; демонстрація ознайомлення з більшістю	3,5-4,4

	запропонованих матеріалів; інформацію подано у вигляді систематизованих висновків з незначними помилками; наявний самостійний розподіл ролей між учасниками команди і вклад кожного у проведення аналітичного огляду; презентація аналітичного огляду відповідно до розподілених ролей.	
	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; наявний розподіл ролей між учасниками команди і вклад кожного у проведення аналітичного огляду; презентація аналітичного огляду відповідно до розподілених ролей.	2,5–3,4
	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; наявний розподіл ролей між учасниками команди, проте нерівномірним є вклад кожного у проведення аналітичного огляду; презентація аналітичного огляду не у відповідності до розподілених ролей або однією людиною.	1,5–3,4
	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; наявний розподіл ролей між учасниками команди, проте нерівномірним є вклад кожного у проведення аналітичного огляду або розподіл ролей відсутній; презентація аналітичного огляду не у відповідності до розподілених ролей або однією людиною.	0,6–1,4
	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; відсутній розподіл ролей між учасниками команди, робота виконувалася самостійно кожним із членів команди без командної взаємодії.	0–0,5
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.	3,5–4

	<p>Змістова відповідність дослідницького проекту 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 проекту; демонстрація вмінь аналізувати та робити висновки з незначними помилками, обґрунтовувати власну позицію.</p>	2,5–3,4
	<p>Часткова змістова відповідність дослідницького проекту 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 проекту із суттєвими помилками; часткова демонстрація вмінь аналізувати та робити висновки із суттєвими помилками, обґрунтовувати власну позицію.</p>	1,5–2,4
	<p>Часткова змістова відповідність дослідницького проекту 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 проекту із суттєвими помилками; допущення суттєвих помилок у вміннях аналізувати та робити висновки, обґрунтовувати власну позицію або невміння аналізувати та робити висновки, обґрунтовувати власну позицію.</p>	0,6–1,4
	<p>Часткова змістова відповідність дослідницького проекту 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 проекту із суттєвими помилками; допущення суттєвих помилок у вміннях аналізувати та робити висновки, обґрунтовувати власну позицію або невміння аналізувати та робити висновки, обґрунтовувати власну позицію.</p>	0–0,5
Анотація наукової статті	<p>Анотація представляє в узагальненому вигляді зміст статті, є інформативною та змістовною. Вона є оригінальною, відсутні прямі повтори будь-яких елементів статті. Для анотації характерні чіткість, логічність та зв'язність викладу. В анотації представлені предмет, тема, мета роботи, результати роботи, висновки.</p>	2,5–3
	<p>Анотація представляє в узагальненому вигляді зміст статті, є інформативною та змістовною. Вона є частково оригінальною, наявна незначна кількість повторів будь-яких елементів статті. Для анотації характерні чіткість, логічність та зв'язність викладу, проте із незначними помилками. В анотації представлені не всі основні</p>	1,5–2,4

	елементи роботи.	
	Анотація представляє в узагальненому вигляді зміст статті, але є недостатньо інформативною та змістовною. Вона є частково оригінальною, наявна значна кількість повторів будь-яких елементів статті. Для анотації характерні чіткість, логічність та зв'язність викладу, проте із помилками. В анотації представлені не всі основні елементи роботи.	0,6–1,4
	Анотація не відповідає змісту статті, або відповідає йому у загальних рисах, не є інформативною та змістовною. В анотації велика кількість повторів будь-яких елементів статті. Для анотації не характерні чіткість, логічність та зв'язність викладу. В анотації представлені не всі основні елементи роботи або не представлені взагалі.	0-0,5
Анотація наукової статті (командна робота)	Анотація представляє в узагальненому вигляді зміст статті, є інформативною та змістовною. Вона є оригінальною, відсутні прямі повтори будь-яких елементів статті. Для анотації характерні чіткість, логічність та зв'язність викладу. В анотації представлені предмет, тема, мета роботи, результати роботи, висновки. Наявний самостійний розподіл ролей між учасниками команди і вклад кожного у виконання анотації; презентація анотації відповідно до розподілених ролей.	2,5–3 / 3,5–4
	Анотація представляє в узагальненому вигляді зміст статті, є інформативною та змістовною. Вона є частково оригінальною, наявна незначна кількість повторів будь-яких елементів статті. Для анотації характерні чіткість, логічність та зв'язність викладу, проте із незначними помилками. В анотації представлені не всі основні елементи роботи. Наявний розподіл ролей між учасниками команди, проте нерівномірним є вклад кожного у виконання анотації; презентація анотації не у відповідності до розподілених ролей або однією людиною.	1,5–2,4 / 2,1–3,4
	Анотація представляє в узагальненому вигляді зміст статті, але є недостатньо інформативною та змістовною. Вона є частково оригінальною, наявна значна кількість повторів будь-яких елементів статті. Для анотації характерні чіткість, логічність та зв'язність викладу, проте із помилками. В анотації представлені не всі основні елементи роботи. Наявний розподіл ролей між учасниками команди, проте нерівномірним є вклад кожного у проведення аналітичного огляду або розподіл ролей відсутній; презентація аналітичного огляду не у відповідності до розподілених ролей або однією людиною.	0,6–1,4 / 0,6–2
	Анотація не відповідає змісту статті, або відповідає йому у загальних рисах, не є інформативною та змістовною. В анотації велика кількість повторів будь-яких елементів статті. Для анотації не характерні чіткість, логічність та зв'язність викладу. В анотації представлені не всі основні елементи роботи або не	0-0,5

	представлені взагалі. Наявний розподіл ролей між учасниками команди, проте нерівномірним є вклад кожного у проведення аналітичного огляду або розподіл ролей відсутній; презентація аналітичного огляду не у відповідності до розподілених ролей або однією людиною.	
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
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. Антонюк А. Б., Русецька В. А. Інтерпол у міжнародній боротьбі з тероризмом. *Юридичний наукових електронний журнал*. 2020. № 7. С. 346–350. URL: http://lsej.org.ua/7_2020/89.pdf (Дата звернення: 22.08.2022).
2. Банк Р. О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право*. 2016. № 1 (16). С. 110–116.
3. Білан І. А. Протидія тероризму: досвід ЄС. *Інформація і право*. 2021. № 2(37). С. 67–73. URL: http://ippi.org.ua/sites/default/files/10_20.pdf (Дата звернення: 22.08.2022).
4. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.
5. Важна К. А. Проблеми визначення поняття й сутності тероризму в міжнародному праві. *Міжнародні відносини: теоретико-практичні аспекти*. 2021. № 8. С. 137–151. doi: <https://doi.org/10.31866/2616-745x.8.2021.249036> (Дата звернення: 22.08.2022).

6. Вейтас М. В., Лукашенко М. І. Кібертероризм: тенденції розвитку та механізми протидії. Науковий огляд. 2018. Том 4. № 47. URL: <https://naukajournal.org/index.php/naukajournal/article/view/1545> (дата звернення: 22.08.2022).
7. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України. *Наукові праці. Політологія*. 2012. Випуск 185. Том 197. URL: <http://lib.chdu.edu.ua/pdf/naukpraci/politics/2012/197-185-15.pdf> (Дата звернення: 22.08.2022).
8. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Ukrainian Scientific Journal of Information Security*. 2013. Vol. 19. Issue 2. С. 118–129.
9. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму. *Часопис Київського університету права*. 2014. № 4. С. 312–317.
10. Громовенко К. В. Сучасні організаційно-правові засади протидії міжнародному тероризму з боку світової спільноти. *Прикарпатський юридичний вісник*. 2021. № 3(38). С. 94–101. URL: http://pjuv.nuoua.od.ua/v3_2021/22.pdf (Дата звернення: 22.08.2022).
11. Гуцалюк М. Кібертероризм та заходи протидії. *Протидія терористичній діяльності: міжнародний досвід і його актуальність для України*: матеріали міжнародної науково-практичної конференції. (30 вересня 2016 року, м. Київ). К.: Національна академія прокуратури України, 2016. С. 86–88.
12. Довгань О. Д., Хлань В. Г. Кібертероризм як загроза інформаційному суверенітету держави. *Інформаційна безпека людини, суспільства, держави*. № 3 (7), 2011. С. 49–53.
13. Михальчук Г. О. Особливості взаємозв'язку сучасного тероризму та засобів масової інформації: теоретичний аспект. *Український психологічний журнал*. 2017. № 2 (4). С. 96–105.
14. Aziz M. H. Counter Terrorism Measures via Internet Intermediaries: A First Amendment & National Security Dilemma. *Journal of Law & Cyber Warfare*. 2015. Vol. 4, No. 2. P. 1-22.
15. Blumbergs B. Technical analysis of advanced threat tactics targeting critical information infrastructure. *Critical information infrastructure*. 2014. URL: <https://ccdcoe.org/uploads/2018/10/2014-Technical-Analysis-of-Advanced-Threat-Tactics-Targeting-Critical-Information-Infrastructure.pdf> (Last Accessed: 22.08.2022).

Допоміжна література

1. 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.
2. Вибухи та захоплення заручників: якими були найгучніші теракти ХХІ століття. 11 вересня 2021 року. *Слово і діло : аналітичний портал*. URL: [Найбільші теракти ХХІ століття - які були наслідки](http://slovo-idilo.org.ua/ua/2021/09/11-vybuchy-ta-zahopennya-zaruchnykiv-yakimi-bu-lyub-nyaj-guchnijshy-terakty-xxi-stolittja-yaki-bu-lyub-naslidky) » *Слово і Діло (slovoidilo.ua)* (Дата звернення: 22.08.2022).
3. Давиденко М. О. Протидія СБ України терористичній пропаганді у інформаційному середовищі України. *Актуальні проблеми управління інформаційною безпекою держави*: збірник тез наук. доп. наук.-практ. конф. (Київ, 4 квітня 2019 р.). Київ: Нац. Акад. СБУ, 2019. С. 35–36. URL: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf (дата звернення: 22.08.2022).
4. 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).
5. Матула М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці. *Науковий блог. Національний університет «Острозька академія»*. 03.07.2014. URL: <https://naub.oa.edu.ua/2014/fenomen-informatsijnoho-teroryzmu-yak-zahrozy-natsionalnij-ta-mizhnarodnij-bezpetsi/> (дата звернення: 22.08.2022).
6. Саган О. В. Протидія медіа-інформаційному тероризму як питання національної безпеки України: дис. ... канд. політ. наук: 21.00.01 / Національний інститут стратегічних досліджень. Київ, 2021. 224 с.
7. 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.

8. 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).

9. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182–186. URL: <http://pgp-journal.kiev.ua/archive/2017/10/38.pdf> (дата звернення: 20.08.2019).

10. 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.

11. Харченко І. М., Сапогов С. О., Шамраєва В. М., Новікова Л. В. Основні засоби інформаційного протидіяння та інформаційної війни як явища сучасного міжнародного політичного процесу. *Вісник Харківського національного університету імені В. Н. Казіна*. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм». 2017. Випуск 6. С. 77–81. URL: <http://international-relations-tourism.karazin.ua/themes/irtb/resources/2c5d772b29c5a9e2139a9f6aa96834d0.pdf> (дата звернення: 20.08.2022).

12. Широкова-Мурараш О. Г., Акчурін Ю. Р. Кіберзлочинність та кібертероризм як загроза міжнародній інформаційній безпеці: міжнародно-правовий аспект. *Інформація і право*. 2011. № 1. С. 76–81.

13. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Науковий вісник Національного університету ДПС України (економіка, право)*. 2014. № 2(65). С. 55–60.

14. Яцик Т. П. Розслідування інформаційного тероризму та кіберзлочинності (міжнародно-правовий аспект). *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія і практика)*. 2017. Вип. 1 (5). С. 111–115.

15. European Commission. «eEurope - An information society for all». URL: http://europa.eu/rapid/press-release_SPEECH-01-180_en.htm?locale=ru (Last Accessed: 22.05.2019).

16. Kumar M. European Union Parliament Under Cyber Attack! *The Hacker News*. March 29, 2011. URL: <https://thehackernews.com/2011/03/european-union-parliament-under-cyber.html> (Last Accessed: 22.08.2019).

17. Lemos R. Cyberterrorism: The Real Risk. *Computer Crime Research Center (CCRC)*. URL: <http://www.crime%research.org/library/Robert1.htm> (дата звернення: 22.08.2019).

18. Petya Ransomware Outbreak: Here's What You Need To Know, Symantec Security Response. *Symantec*. 24 October, 2017. URL: <https://www.symantec.com/blogs/threat-intelligence/petya-ransomware-wiper> (Last Accessed: 22.08.2022).

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. ІНТЕРПОЛ – <https://www.interpol.int/>
17. European Union Agency For Cybersecurity (ENISA) – <https://www.enisa.europa.eu/>
18. Computer Emergency Response Team of Ukraine (CERT-UA) – <https://cert.gov.ua/>
19. ЄВРОПОЛ – <https://www.europol.europa.eu/about-europol>
20. 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 доступу: 620976) проводяться всі лекційні та практичні (семінарські) заняття, а також завдання для роботи на практичних (семінарських) заняттях та самостійної роботи виконуються на платформі moodle (<https://moodle.karazin.ua/course/view.php?id=5794>)

Додаток до робочої програми навчальної дисципліни «Інформаційний тероризм»

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.