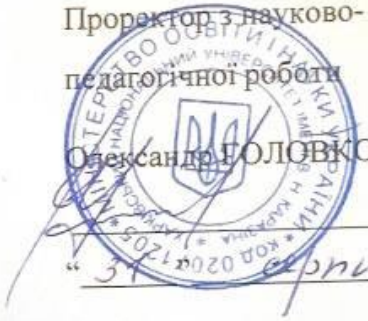
Міністерство освіти і науки України

Харківський національний університет імені В.Н. Каразіна

Кафедра міжнародних відносин, міжнародної інформації та безпеки

"ЗАТВЕРДЖУЮ"

Проректор з науково-
педагогічної роботи
Олександр ГОЛОВКО



"____" _____ 2022р.

Робоча програма навчальної дисципліни

Захист національного інформаційного простору

рівень вищої освіти другий (магістерський)
галузь знань 29 «Міжнародні відносини»
спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
освітня програма «Міжнародна інформаційна безпека»
вид дисципліни обов'язкова
факультет Міжнародних економічних відносин та туристичного бізнесу

2022 / 2023 навчальний рік

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

"___30____"_____08_____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__"____08_____2022 року № _1___

Завідувач кафедри міжнародних відносин, міжнародної інформації та безпеки

_____ Людмила НОВІКОВА
(підпис) (прізвище та ініціали)

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

Гарант освітньої програми «Міжнародна інформаційна безпека»

Людмила НОВІКОВА

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

Протокол від "_29___"_____08_____2022 року № _1___

Голова науково- методичної комісії_____

_____ Лариса ГРИГОРОВА-БЕРЕНДА
(підпис) (прізвище та ініціали)

ВСТУП

Програма навчальної дисципліни «Захист національного інформаційного простору» 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 з основних засад захисту національного інформаційного простору України як чинника національної безпеки, а також практичних умінь та навичок правильного тлумачення та застосування заходів інформаційної протидії, 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 8. Здатність виявляти ініціативу та підприємливість.

ЗК 9. Здатність оцінювати та забезпечувати якість виконуваних робіт.

- 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 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 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.	-
у тому числі індивідуальні завдання	
- год.	-

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

2. Тематичний план навчальної дисципліни

Розділ 1. Загальні засади захисту національного інформаційного простору

Тема 1. Концепція інформаційного суспільства

- основні положення Окінавської хартії глобального інформаційного суспільства 2000 року;
- ключові принципи інформаційного суспільства згідно з Декларацією принципів «Побудова інформаційного суспільства – глобальне завдання у новому тисячолітті» 2003 року;
- основні напрями дій, спрямованих на побудову інформаційного суспільства, відповідно до Женевського плану дій 2001 року;
- основні положення Туніського зобов'язання 2005 року;
- основні положення Туніської програми для інформаційного суспільства 2005 року;

Тема 2. Стан розвитку інформаційного суспільства в Україні

- завдання, цілі та напрями розвитку інформаційного суспільства в Україні;
- національна політика розвитку інформаційного суспільства в Україні;
- організаційно-правові основи розвитку інформаційного суспільства в Україні;
- стратегія розвитку інформаційного суспільства в Україні.

Тема 3. Загальна характеристика національного інформаційного простору

- поняття, структура та функції інформаційного простору;
- поняття та ознаки національного інформаційного простору.

Тема 4. Інформаційна безпека в контексті національної безпеки

- поняття та сутність національної безпеки держави;
- основні положення закону України «Про національну безпеку України» 2018 року;

- Стратегія національної безпеки України 2020 року;
- Доктрина інформаційної безпеки України 2016 року;
- Стратегія кібербезпеки України 2021 року;
- Стратегія інформаційної безпеки України 2021 року.

Тема 5. Інституційно-правові інструменти захисту національного інформаційного простору України

- основні нормативно-правові акти у сфері захисту національного інформаційного простору;
- основні інституції України, що мають повноваження у сфері захисту національного інформаційного простору.

Розділ 2. Окремі аспекти захисту національного інформаційного простору

Тема 6. Захист таємної та конфіденційної інформації в Україні

- становлення та розвиток інституту захисту інформації в Україні;
- становлення державних органів, що захищають державну таємницю;
- законодавче регулювання обігу таємної інформації в Україні;
- поняття та захист службової інформації з обмеженим доступом;
- поняття та захист професійних таємниць.

Тема 7. Дезінформація як загроза національному інформаційному простору України в сучасних умовах

- поняття, основні інструменти та тактики дезінформації;
- фейк як інструмент побудови наративу;
- практичні загрози дезінформації в Україні.

Тема 8. Досвід захисту національного інформаційного простору в інших країнах

- захист національного інформаційного простору у США;
- захист національного інформаційного простору у країнах Європи;
- захист національного інформаційного простору у країнах Азії.

Тема 9. Інформаційна гігієна в сучасних умовах в Україні

- поняття та правила інформаційної гігієни;
- пропаганда та інформаційно-психологічні операції в національному інформаційному просторі України.

3. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	с	лаб	інд.	с.р.		л	с	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Загальні засади захисту національного інформаційного простору												
Тема 1. Концепція інформаційного суспільства	19	4	1	-	-	14	-	-	-	-	-	-
Тема 2. Стан розвитку інформаційного суспільства в Україні	18	2	2	-	-	14	-	-	-	-	-	-
Тема 3. Загальна характеристика національного інформаційного	22	2	2	-	-	18	-	-	-	-	-	-

простору												
Тема 4. Інформаційна безпека в контексті національної безпеки	13	4	1	-	-	8	-	-	-	-	-	-
Тема 5. Інституційно-правові засади захисту національного інформаційного простору України	27	4	2	-	-	21	-	-	-	-	-	-
Разом за розділом 1	**99**	**16**	**8**	**-**	**-**	**75**	**-**	**-**	**-**	**-**	**-**	**-**
Розділ 2. Окремі аспекти захисту національного інформаційного простору												
Тема 6. Захист таємної та конфіденційної інформації в Україні	28	6	2	-	-	20	-	-	-	-	-	-
Тема 7. Дезінформація як загроза національному інформаційному простору України в сучасних умовах	16	4	2	-	-	10	-	-	-	-	-	-
Тема 8. Досвід захисту національного інформаційного простору в інших країнах	27	4	2	-	-	21	-	-	-	-	-	-
Тема 9. Інформаційна гігієна в сучасних умовах в Україні	10	2	2	-	-	6	-	-	-	-	-	-
Разом за розділом 2	**81**	**16**	**8**	**-**	**-**	**57**	**-**	**-**	**-**	**-**	**-**	**-**
Усього годин	**120**	**32**	**16**	**-**	**-**	**132**	**-**	**-**	**-**	**-**	**-**	**-**

4. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	Тема 1. Концепція інформаційного суспільства	1
2	Тема 2. Стан розвитку інформаційного суспільства в Україні	2
3	Тема 3. Загальна характеристика національного інформаційного простору	2
4	Тема 4. Інформаційна безпека в контексті національної безпеки	1
5	Тема 5. Інституційно-правові засади захисту національного інформаційного простору України	2
6	Тема 6. Захист таємної та конфіденційної інформації в Україні	2
7	Тема 7. Дезінформація як загроза національному інформаційному простору України в сучасних умовах	2
8	Тема 8. Досвід захисту національного інформаційного простору в інших країнах	2
9	Тема 9. Інформаційна гігієна в сучасних умовах в Україні	2

	Разом	**16**

5. Завдання для самостійної роботи

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	**Тема 1. Концепція інформаційного суспільства** *Завдання:* 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Захист національного інформаційного простору» https://moodle.karazin.ua/course/view.php?id=3878 , Тема 1) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (7 год). 2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на семінарському занятті: 1) Західний тип побудови інформаційного суспільства; 2) Азійський тип побудови інформаційного суспільства (7 год.).	14
2	**Тема 2. Стан розвитку інформаційного суспільства в Україні** *Завдання:* 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Захист національного інформаційного простору» https://moodle.karazin.ua/course/view.php?id=3878 , Тема 2) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті, а також до розв'язання тестових завдань (7 год). 2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на семінарському занятті: 1) Електронне урядування в Україні; 2) Е-демократія в Україні; 3) Е-економіка в Україні; 4) Е-освіта в Україні; 5) Е-медицина в Україні (7 год.).	14
3	**Тема 3. Загальна характеристика національного інформаційного простору** *Завдання:* 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Захист національного інформаційного простору» https://moodle.karazin.ua/course/view.php?id=3878 , Тема 3) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (6 год). 2. Ознайомитися з науковою статтею http://pgp-journal.kiev.ua/archive/2018/5/27.pdf та підготувати анотацію (5 год). 3. Підготувати аналітичний огляд на тему: «Порівняльна характеристика інформаційного та кіберпростору», представити у вигляді таблиці (7 год.).	18
4	**Тема 4. Інформаційна безпека в контексті національної безпеки** *Завдання:* 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Захист національного інформаційного простору» https://moodle.karazin.ua/course/view.php?id=3878 , Тема 4) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті, а також до	8

	розв’язання тестових завдань (8 год).	
5	**Тема 5. Інституційно-правові засади захисту національного інформаційного простору України** *Завдання:* 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Захист національного інформаційного простору» https://moodle.karazin.ua/course/view.php?id=3878 , Тема 5) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (7 год). 2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на семінарському занятті: 1) Роль Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв’язку та захисту інформації України, а також його спеціалізованого структурного підрозділу CERT-UA у сфері захисту національного інформаційного простору України; 2) Роль Служби безпеки України у сфері захисту національного інформаційного простору України; 3) Роль Департаменту кіберполіції Національної поліції України у сфері захисту національного інформаційного простору України; 3) Роль Державної служби спеціального зв'язку та захисту інформації України у сфері захисту національного інформаційного простору України (7 год.). 3. Підготувати аналітичний огляд на одну з наступних тем (на вибір): 1) «Основні інституції в Україні, що мають повноваження у сфері захисту національного інформаційного простору, та їх функції»; 2) «Основні нормативно-правові акти України у сфері захисту національного інформаційного простору», представити у вигляді таблиці (7 год.).	21
6	**Тема 6. Захист таємної та конфіденційної інформації в Україні** *Завдання:* 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Захист національного інформаційного простору» https://moodle.karazin.ua/course/view.php?id=3878 , Тема 6) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті, а також до розв’язання тестових завдань (13 год). 2. Підготувати дослідницький проєкт на одну з наступних тем (на вибір) та підготуватися до його захисту на семінарському занятті: 1) Охорона інтелектуальної власності в світі (обрати країну самостійно); 2) Охорона інтелектуальної власності в Україні; 3) Охорона персональних даних в світі (обрати країну самостійно); 4) Охорона персональних даних в Україні (7 год.).	20
7	**Тема 7. Дезінформація як загроза національному інформаційному простору України в сучасних умовах** *Завдання:* 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Захист національного інформаційного простору» https://moodle.karazin.ua/course/view.php?id=3878 , Тема 7) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (10 год).	10

8	**Тема 8. Досвід захисту національного інформаційного простору в інших країнах** *Завдання:* 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Захист національного інформаційного простору» https://moodle.karazin.ua/course/view.php?id=3878 , Тема 8) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (7 год). 2. Підготувати дослідницький проєкт на тему: «Особливості захисту національного інформаційного простору в певній країні світу» (обрати країну самостійно) (7 год.). 3. Підготувати аналітичний огляд на тему: «Порівняльна характеристика захисту національного інформаційного простору в Україні та в країнах ЄС», представити у вигляді таблиці (7 год.).	21
9	**Тема 9. Інформаційна гігієна в сучасних умовах в Україні** *Завдання:* 1. Ознайомитися з лекційним матеріалом, рекомендованою літературою та інформаційними ресурсами за темою (Дистанційний курс «Захист національного інформаційного простору» https://moodle.karazin.ua/course/view.php?id=3878 , Тема 9) та підготуватися до усного опитування та навчальної дискусії за навчальними питаннями на семінарському занятті (6 год).	6
	Разом	**132**

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 «Захист національного інформаційного простору»

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	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття); дослідницький проєкт; аналітичний огляд.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду.

	відносинах.		
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; анотація на наукову статтю.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; 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 семінарського заняття); дослідницький проєкт; аналітичний огляд.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду.
РН 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 семінарського заняття); дослідницький проєкт; аналітичний огляд.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; тестування.
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; анотація на наукову статтю.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання анотації на наукову статтю; тестування.
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; анотація на наукову статтю.	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання анотації на наукову статтю; тестування.
РН 22	Демонструвати здатність до подальшого навчання з високим	Лекція-візуалізація; усне опитування; навчальна дискусія (за питаннями семінарського заняття);	Оцінювання усної відповіді здобувача та виступу під час навчальної дискусії (за питаннями семінарського

	рівнем автономності.	дослідницький проєкт; аналітичний огляд; анотація на наукову статтю.	заняття); оцінювання захисту дослідницького проєкту; оцінювання аналітичного огляду; оцінювання анотації на наукову статтю; 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 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; 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 семінарському занятті здобувач може отримати від 3 до 10 балів. Загальна сума балів за виконання завдань для самостійної роботи та роботу на семінарських заняттях 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										Екзамен	Сума
Розділ 1					Розділ 2				Разом		
Т1	Т2	Т3	Т4	Т5	Т6	Т7	Т8	Т9	60	40	100
7	8	9	4	9	7	3	10	3			

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.	**2,5–3**
	Середня здобувача на 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 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 семінарському занятті, демонстрація незасвоєння матеріалу теми, неознайомлення чи ознайомлення з незначною частиною запропонованих джерел, неуміння робити висновки.	**0-0,5**
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.	**2,6–3**
	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	**2–2,5**

	помилками.	
	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.	**1,5–1,9**
	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.	**1–1,4**
	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.	**0,5–0,9**
	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.	**0-0,5\4**
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**
	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.	**2,5–3,4**
	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.	**1,5–2,4**
	Часткова змістовна відповідність дослідницького	**0,6–1,4**

	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.	
	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.	**0–0,5**
Анотація наукової статті	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.	**2,5–3**
	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.	**1,5–2,4**
	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.	**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**
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	Здобувач правильно відповів на всі тестові питання.	**40**

контроль (тестування)	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. Бусол О. Інформаційна безпека США: законодавче регулювання та перспективи співпраці для України. Центр соціальних комунікацій НБУВ. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2988:informatsijnabezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlyaukrajini&catid=8&Itemid=350 (дата звернення: 20.08.2022).
2. Бусол О. Основні риси контролю за національним інформаційним простором Королівства Велика Британія. Центр соціальних комунікацій НБУВ. URL: http://nbuviap.gov.ua/index.php?option=com_content&view=article&id=2962:osnovni-risikontrolyu-za-natsionalnim-informatsijnim-prostorom-korolivstva-velika-britaniya2&catid=71&Itemid=382 (дата звернення: 20.08.2022).
3. Дубняк К. А. Інформаційний простір: структура та функціональні параметри. *Держава та регіони. Серія: Соціальні комунікації.* 2015. № 4 (24). С. 21–25.
4. Косогов О. М., Сірик А. О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на сході України. *Системи озброєння і військова техніка.* 2017. № 1 (49). С. 38–41.
5. Лапінська Є. І. Інформаційна безпека: поняття, види та ознаки. *Порівняльно-аналітичне право.* 2018. № 6. С. 262–266.
6. 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).
7. Політанський В. С. Світові моделі та фундаментальні принципи інформаційного суспільства. *Науковий вісник Ужгородського національного університету. Серія Право.* Випуск 43. Том 1. С. 34–39. URL: http://www.visnykjuris.uzhnu.uz.ua/file/No.43/part_1/10.pdf (дата звернення: 20.08.2022).
8. Попова Т. Захист національного інформаційного простору. Досвід США для України. *Радіо Свобода.* 02 листопада 2017. URL: https://www.radiosvoboda.org/a/28830390.html (дата звернення: 20.08.2022).

9. Семенов А. Захист національного інформаційного простору Великої Британії. *Політична праксеологія: безпека, технології, комунікації:* Матеріали міжнародної конференції. За ред. В. Бебика. Київ: ВАПН, 2016. С. 91–93.

10. Солдатенко О. Інформаційний простір у мережі Інтернет: правове регулювання та контроль. *Адміністративне право і процес.* 2018. № 5. С. 134–140. URL: http://pgpjournal.kiev.ua/archive/2018/5/27.pdf (дата звернення: 20.08.2022).

11. Солодка О. М. Захист інформаційного простору України в умовах інформаційного суспільства. Місце і роль бібліотек у формуванні національного інформаційного простору: матеріали міжнародної наукової конференції, м. Київ, 21–23 жовтня 2014 року. URL: http://conference.nbuv.gov.ua/report/view/id/406 (дата звернення: 20.08.2022).

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. Шевченко М. Поняття національного інформаційного простору та його характеристики. Теорія і практика сучасної журналістики. *Український інформаційний простір.* 2018. Випуск 1. С. 103–112.

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.

19. What is the Difference between Cyber Security and Information Security? Computer Science Degree Hub. URL: https://www.computersciencedegreehub.com/faq/what-is-thedifference-between-cyber-security-and-information-security / (Last Accessed: 20.08.202).

20. Wyss W. Cybersecurity in Switzerland. February 24, 2020. LEXOLOGY : web-site. URL: https://www.lexology.com/library/detail.aspx?g=67fa41c8-03f1-44d7-a55f-d291c021a30a (Last Accessed: 20.08.202).

Допоміжна література

1. Головка А. А. Громадянське суспільство як суб'єкт протидії загрозам національній безпеці в інформаційній сфері : дис. …канд. політ. наук : 21.01.01. Київ, 2018. 199 с.

2. Бондар Ю. В. Становлення та еволюція національного інформаційного простору України в процесі формування демократичної політичної культури українського суспільства: автореф. дис. …канд. політ. наук: 23.0.03/ Національний педагогічний університет імені М. П. Драгоманова. Київ, 2010. 20 с.

3. Буньківська О. В. Інформаційний простір: соціокультурна сутність, стан та проблеми функціонування в Україні: автореф. дис. …канд. культурології: 26.00.01 / Київський національний університет культури і мистецтв. Київ, 2009. 23 с.

4. 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.

5. Валюшко І. О. Інформаційна безпека України в контексті російськоукраїнського конфлікту: дис. … канд. політ. наук: 23.00.04 / Дипломатична академія України при МЗС України; Чорноморський національний університет імені Петра Могили. Київ, 2018. 210 с.

6. Войціховський А. В. Забезпечення безпеки інформаційного простору як напрям правоохоронної діяльності ООН. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2015. № 2. С. 76–85. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/2199/zabezpechennya_bezpeki_informaciynogo_pr.pdf?sequence=2&isAllowed=y (дата звернення: 20.08.2022).

7. Демченко м. А. Специфіка формування національного інформаційного простору в сучасній Україні в контексті зміни державної політики в інформаційній галузі. Наукові праці МАУП. 2016. Вип. 49 (2). С. 43–46.

8. Куцька О.М. Особливості інформаційно-психологічного впливу Російської Федерації напередодні та початковому етапі антитерористичної операції на сході України. *Інформаційна безпека людини, суспільства, держави.* 2017. № 1(21). С. 180–190.

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

10. 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.

11. 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.

12. Collins A. Contemporary Security Studies. 3rd ed. United Kingdom: Oxford University Press, 2013. 478 p.

13. 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).

14. Potts M. The State Information Security. Network Security. 2012. Volume 2012. Issue 7. P. 9–11. URL: https://www.sciencedirect.com/science/article/pii/S1353485812700648 (Last Accessed: 20.08.2022).

15. What is Information Security? URL: https://warwick.ac.uk/services/idc/informationsecurity/training/info_sec_quick_guide.pdf (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. Computer Emergency Response Team of Ukraine (CERT-UA) – https://cert.gov.ua/
17. 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=3877)

Додаток 1

Додаток до робочої програми навчальної дисципліни «Захист національного інформаційного простору»

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.