

Міністерство освіти і науки України

Харківський національний університет імені В. Н. Каразіна

Кафедра міжнародних відносин, міжнародної інформації та безпеки

«ЗАТВЕРДЖУЮ»

Проректор з науково-педагогічної роботи

Антон ПАНТЕЛЕЙМОНОВ



08. 2020 р.

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: за вибором

факультет міжнародних економічних відносин та туристичного бізнесу

2020 / 2021 навчальний рік

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

«28» серпня 2020 року, протокол № 1

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

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

Протокол від «26» серпня 2020 року № 1

Завідувач кафедри


(підпис)

Людмила НОВІКОВА
(ім'я та прізвище)

Програму погоджено з гарантом освітньо-професійної програми

«Міжнародна інформаційна безпека»
назва освітньої програми

Гарант освітньо-професійної програми

«Міжнародна інформаційна безпека»

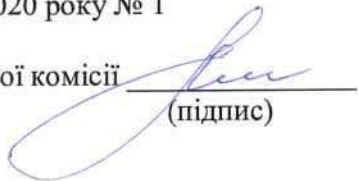

(підпис)

Людмила НОВІКОВА
(ім'я та прізвище)

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

Протокол від «28» серпня 2020 року № 1

Голова навчально-методичної комісії


(підпис)

Лариса ГРИГОРОВА-БЕРЕНДА
(ім'я та прізвище)

ВСТУП

Програма навчальної дисципліни «Захист національного інформаційного простору» складена відповідно до освітньо-професійної програми «Міжнародна інформаційна безпека» підготовки магістра спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії».

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни полягає у формуванні у здобувачів базових знань 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 комплексних теоретичних та практичних задач під час їх майбутньої професійної діяльності у галузі міжнародних відносин, зовнішньої політики, міжнародних комунікацій та регіональних студій та при проведенні досліджень.

1.2. Основні завдання вивчення дисципліни:

- формування наступних загальних компетентностей:

ЗК 7. Уміння аргументувати вибір шляхів вирішення завдань професійного характеру, критично оцінювати отримані результати та обґрунтовувати прийняті рішення.

ЗК 11. Навички міжособистісної взаємодії, цінування та повага різноманітності та багатокультурності, здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань/видів діяльності).

- формування наступних фахових компетентностей:

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

ФК 8. Здатність організовувати та проводити міжнародні зустрічі та переговори, працювати в рамках міжнародних конференцій, організацій, інших форм практичного співробітництва, працювати з дипломатичними міжнародними документами.

ФК 11. Здатність виробляти підходи до розв'язання проблем і завдань у сфері міжнародних відносин, міжнародної та національної безпеки, зовнішньої політики (зокрема міжнародних та внутрішньодержавних конфліктів).

1.3. Кількість кредитів – 3

1.4. Загальна кількість годин – 90

1.5. Характеристика навчальної дисципліни	
За вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2-й	-й
Семестр	
3-й	-й
Лекції	
10 год.	год.
Практичні заняття	
10 год.	год.
Лабораторні заняття	

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

2. Заплановані результати навчання:

Згідно з вимогами освітньо-професійної програми матриця відповідності освітнього компонента **ВБ 1.4. «Захист національного інформаційного простору»**, методів навчання та форм оцінювання, які використовуються, програмним результатам навчання, визначеним освітньо-професійною програмою «Міжнародна інформаційна безпека».

Результати навчання	Методи навчання	Форми оцінювання
ПРН 32 – знання методичних основ та технологій здійснення інформаційно-психологічних операцій в міжнародних відносинах.	Пояснювально-ілюстративний, пояснювально-рецептивний, репродуктивний, проблемний виклад, евристичний, проблемно-пошуковий, дослідницький, метод оволодіння новими знаннями, методи стимулювання інтересу до навчання, методи контролю та корекції за ефективністю навчально-пізнавальної діяльності, а також методи дистанційного навчання та оцінювання на платформах Moodle, Zoom або Google Meet.	Підготовка відповідей за навчальними питаннями теми, усне опитування та навчальні дискусії; виконання тестових завдань; підготовка та захист презентацій доповідей; підготовка тематичних схем; підготовка та захист есе; аналіз наукових статей та нормативних актів та навчальні дискусії за науковими статтями та нормативними актами, розробка, презентація та захист порівняльних таблиць, групова робота з підготовки питань для колоквіуму, колоквіум.
ПРН 42 – знання теоретичних та практичних основ забезпечення інформаційної безпеки держави.	-/-	-/-
ПРН 40 – володіти теоретичними та практичними основами забезпечення інформаційної безпеки держави.	-/-	-/-
ПРН 47 – мати практичні навички із забезпечення інформаційної безпеки держави.		

3. Тематичний план навчальної дисципліни

Розділ 1. Загальні засади захисту національного інформаційного простору

Тема 1. Теоретичні засади національного інформаційного простору.

Концепція інформаційного суспільства. Стан розвитку інформаційного суспільства в Україні. Поняття інформаційного простору та інформаційної сфери. Поняття та основні характеристики національного інформаційного простору.

Тема 2. Інформаційна безпека в контексті національної безпеки держави.

Поняття та сутність національної безпеки держави. Стратегія національної безпеки України. Поняття та сутність інформаційної безпеки держави. Доктрина інформаційної безпеки України.

Тема 3. Інституційно-правові засади захисту національного інформаційного простору України.

Основні правові акти України у сфері захисту національного інформаційного простору. Основні інституції України, що мають повноваження у сфері захисту національного інформаційного простору.

Тема 4. Досвід захисту національного інформаційного простору в інших країнах.

Захист національного інформаційного простору в США. Захист національного інформаційного простору в країнах Європи. Захист національного інформаційного простору в країнах Азії.

4. Структура навчальної дисципліни

Назви розділів і тем	Кількість годин											
	денна форма						заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб.	інд.	с. р.		л	п	лаб.	інд.	с. р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Розділ 1. Загальні засади захисту національного інформаційного простору												
Тема 1. Теоретичні засади національного інформаційного простору	20	2	2	-	-	16	-	-	-	-	-	-
Тема 2. Інформаційна безпека в контексті національної безпеки держави	18	2	2	-	-	14	-	-	-	-	-	-
Тема 3. Інституційно-правові засади захисту національного інформаційного простору України	22	2	2	-	-	18	-	-	-	-	-	-

Тема 4. Досвід захисту національного інформаційного простору в інших країнах	30	4	4	-	-	22	-	-	-	-	-	-
Усього годин	90	10	10	-	-	70	-	-	-	-	-	-

5. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Теоретичні засади національного інформаційного простору	2
2	Інформаційна безпека в контексті національної безпеки держави	2
3	Інституційно-правові засади захисту національного інформаційного простору України	2
4	Досвід захисту національного інформаційного простору в інших країнах	4
	Разом	10

6. Завдання для самостійної роботи

№ з/п	Назва теми та зміст самостійної роботи	Кількість годин
1	Теоретичні засади національного інформаційного простору. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття; підготувати презентації доповідей на визначену тему (на вибір); ознайомитися та проаналізувати наукові статті; розробити порівняльну таблицю.	16
2	Інформаційна безпека в контексті національної безпеки держави. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття; ознайомитися та проаналізувати наукову статтю; ознайомитися та проаналізувати нормативний акт; підготувати тематичну схему.	14
3	Інституційно-правові засади захисту національного інформаційного простору України. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття; підготувати презентації доповідей на визначену тему (на вибір); підготувати тематичну схему; підготувати есе.	18
4	Досвід захисту національного інформаційного простору в інших країнах. <i>Завдання:</i> ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими	22

	відповідати на усні запитання за навчальними питаннями практичного заняття; підготувати презентації доповідей на визначену тему (на вибір); підготувати есе; розробити порівняльну таблицю; поділитися на дві групи та підготувати питання здобувачам іншої групи за всіма темами курсу для колоквіуму.	
	Разом	70

7. Індивідуальні завдання

Не передбачено.

8. Методи контролю

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

Сума балів за виконання завдань на практичному занятті складає:

Тема 1 – 5,5 балів: (виконання тестових завдань – 1 бал, захист презентацій доповідей – 1 бал; навчальна дискусія за науковими статтями – 3 бали; презентація та захист порівняльної таблиці – 0,5 бал).

Тема 2 – 4 бали: (виконання тестових завдань – 1 бал; навчальна дискусія за науковою статтею – 1,5 бали; навчальна дискусія за нормативним актом – 1,5 бали).

Тема 3 – 4,5 бали: (виконання тестових завдань – 1 бал, захист презентацій доповідей – 1 бал; навчальна дискусія за науковою статтею – 1,5 бали; захист есе – 1 бал).

Тема 4 – 10 балів: (захист презентацій доповідей – 2 бали (1 за кожену презентацію); презентація та захист порівняльної таблиці – 2; захист есе – 1 бал; колоквіум – 5).

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

Сума балів за виконання завдань для самостійної роботи здобувачів складає:

Тема 1 – 8 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; підготовка презентацій доповідей – 2 бали; аналіз наукових статей – 3 бали; розробка порівняльної таблиці – 1 бал.

Тема 2 – 6 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; аналіз наукової статті – 1,5 бали; аналіз нормативного акту – 1,5 бали; підготовка тематичної схеми – 1 бал.

Тема 3 – 8 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; підготовка презентацій доповідей – 2 бали; підготовка тематичної схеми – 2 бали (1 за кожену схему); підготовка есе – 2 бали.

Тема 4 – 14 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; підготовка презентацій доповідей – 4 бали; розробка порівняльної таблиці – 2 бали; підготовка есе – 2 бали; групова робота з підготовки питань до колоквіуму – 4.

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

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

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

У разі настання / подовження дії **обставин непоборної сили** (в тому числі запровадження жорстких карантинних обмежень в умовах пандемії з заборотою відвідування ЗВО) здобувачам вищої освіти денної та заочної форм навчання надається можливість скласти залік **у такій самій формі дистанційно на платформі Moodle** в дистанційному курсі «Захист національного інформаційного простору».

9. Схема нарахування балів

Поточний контроль, самостійна робота, індивідуальні завдання				Разом	Залікова робота	Сума
Розділ 1						
T1	T2	T3	T4	60	40	100
13,5	10	12,5	24			

T1, T2 ... – теми розділів.

Критерії оцінки успішності та результатів навчання

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

Розрахункова шкала для оцінювання роботи здобувачів за поточним контролем.

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

37–43	Наявність пропущених лекцій та практичних занять, відпрацювання тем пропущених практичних занять, виконання завдань до кожного практичного заняття, активна робота на практичних заняттях, засвоєння основних положень курсу, допущення декількох незначних помилок при виконанні завдань, здатність визначення теоретичних питань, на які розраховані завдання, здатність публічно представити матеріал.
29–36	Наявність пропущених лекцій та практичних занять, відпрацювання тем пропущених та практичних занять, епізодична відсутність виконання завдань, участь у роботі на практичних заняттях, засвоєння окремих положень матеріалу, неповні відповіді при виконанні завдань, складності при визначенні теоретичних питань, на які розраховані завдання, здатність публічно представити матеріал.
21–28	Несистематичне відвідування лекцій та практичних занять, відсутність на заняттях без поважних причин, наявність декількох невідпрацьованих тем пропущених практичних занять, епізодична відсутність виконаних завдань, участь у роботі на практичних заняттях, засвоєння окремих положень матеріалу тем змістовного розділу, неповні відповіді, допущення помилок при виконанні завдань, великі складності при визначенні теоретичних питань на які розраховані завдання, невпевнені навички публічного представлення матеріалу.
13-20	Епізодичне відвідування лекцій та практичних занять, відсутність на заняттях без поважної причини, наявність невідпрацьованих тем пропущених лекцій та практичних занять, епізодична відсутність виконаних завдань, пасивна робота на практичних заняттях (участь у роботі останніх лише за наявності стимулу з боку викладача), наявність певного уявлення щодо матеріалу тем змістовного розділу, неповні відповіді, допущення значної кількості помилок при виконання завдання, невміння визначити теоретичні питання, на які розраховано завдання, невпевнені навички публічного представлення матеріалу.
6-12	Систематичні пропуски лекцій та практичних занять без поважних причин, наявність невідпрацьованих тем пропущених лекцій та практичних занять, систематична відсутність виконаних завдань, пасивність у роботі на практичних заняттях, неповні, необґрунтовані відповіді, допущення істотних помилок при виконанні завдань, нездатність визначити теоретичні питання, на які розраховані завдання.
0-5	Систематичні пропуски лекцій та практичних занять без поважних причин, теми пропущених лекцій та практичних занять не відпрацьовані, систематична відсутність виконаних завдань, пасивність у роботі на практичних заняттях, відсутність знань, неповні, необґрунтовані відповіді, допущення істотних помилок при виконанні завдання, нездатність визначити теоретичні питання, на які розраховані завдання, невміння публічно представити матеріал, порушення норм академічної доброчесності при виконанні завдань.

Результати оцінювання роботи здобувачів фіксуються у відповідній відомості.

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

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

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

Кількість балів	Критерії оцінювання
40	Здобувач правильно відповів на всі тестові питання.
30	Здобувач правильно відповів на не менш, ніж 75 % тестових питань.
20	Здобувач правильно відповів на не менш, ніж 50 % тестових питань.
10	Здобувач правильно відповів на не менш ніж 25 % тестових питань.
0	Здобувач не відповів на жодне з тестових питань.
Правильна відповідь на одне тестове питання – 1 бал.	

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90–100	відмінно	зараховано
70–89	добре	
50–69	задовільно	
1–49	незадовільно	не зараховано

10. Рекомендована література

Основна література

1. Бурячок В. Л. Основи формування державної системи кібернетичної безпеки: монографія / В. Л. Бурячок. К.: НАУ, 2013. 432 с.
2. 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:informatsijna-bezpeka-ssha-zakonodavche-regulyuvannya-ta-perspektivi-spivpratsi-dlya-ukrajini&catid=8&Itemid=350 (дата звернення: 20.08.2020).
3. 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-risi-kontrolyu-za-natsionalnim-informatsijnim-prostorom-korolivstva-velika-britaniya-2&catid=71&Itemid=382 (дата звернення: 20.08.2020).
4. 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.
5. Декларація принципів «Побудова інформаційного суспільства - глобальне завдання у новому тисячолітті»: Міжнародний документ від 12 грудня 2003 року. URL: https://zakon.rada.gov.ua/laws/show/995_c57 (дата звернення: 20.08.2020).
6. Дубняк К. А. Інформаційний простір: структура та функціональні параметри. Держава та регіони. Серія: Соціальні комунікації. 2015. № 4 (24). С. 21–25.

7. Женевський план дій від 12 грудня 2003 року. *Асоціація підприємств інформаційних технологій України*. URL: <http://old.apitu.org.ua/wsis/pd> (дата звернення: 22.05.2019).

8. 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.

9. Лапінська Є. І. Інформаційна безпека: поняття, види та ознаки. Порівняльно-аналітичне право. 2018. № 6. С. 262–266.

10. 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: 03.05.2020).

11. Окінавська хартія глобального інформаційного суспільства: Міжнародний документ від 22 липня 2000 року. URL: https://zakon.rada.gov.ua/laws/show/998_163 (дата звернення: 20.08.2020).

12. 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.visnyk-juris.uzhnu.uz.ua/file/No.43/part_1/10.pdf (дата звернення: 20.08.2020).

13. 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: 20.08.2020).

14. Про інформацію: Закон України від 02 жовтня 1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#n18> (дата звернення: 20.08.2020).

15. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> (дата звернення: 20.08.2020).

16. Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 09 січня 2007 року № 537-V. URL: <https://zakon.rada.gov.ua/laws/show/537-16> (дата звернення: 20.08.2020).

17. Про рішення Ради національної безпеки і оборони України від 06 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 року № 287/2015. URL: <https://zakon.rada.gov.ua/laws/show/287/2015> (дата звернення: 20.08.2020).

18. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 року № 247/2017. URL: <https://zakon.rada.gov.ua/laws/show/47/2017> (дата звернення: 20.08.2020).

19. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінету міністрів України від 15 травня 2013 року № 386-р. URL: <https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80/ed20130515#n21> (дата звернення: 20.08.2020).

20. 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.

21. Солдатенко О. Інформаційний простір у мережі Інтернет: правове регулювання та контроль. *Адміністративне право і процес*. 2018. № 5. С. 134–140. URL: <http://pgp-journal.kiev.ua/archive/2018/5/27.pdf> (дата звернення: 20.08.2020).

22. 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: 20.08.2020).

23. 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: 20.08.2020).
24. 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: 20.08.2020).
25. Туніська програма для інформаційного суспільства від 18 листопада 2005 року. *Інформаційне суспільство в Україні*. URL: https://informationsociety.wordpress.com/basics/BCIC_outcomes/tp/#C (дата звернення: 20.08.2020).
26. Туніське зобов'язання з питань інформаційного суспільства від 18 листопада 2005 року. *Асоціація підприємств інформаційних технологій України*. URL: <http://old.apitu.org.ua/BCIC/tz> (дата звернення: 20.08.2020).
27. Шевченко М. Поняття національного інформаційного простору та його характеристики. *Теорія і практика сучасної журналістики. Український інформаційний простір*. 2018. Випуск 1. С. 103–112.
28. 2019 China Data Protection & Cybersecurity Annual Report. March 2020. URL: <https://www.dentons.com/en/insights/guides-reports-and-whitepapers/2020/march/31/-/media/ae0259f3ddf14fecb5b3ceb1c25aaec8.ashx> (Last Accessed: 20.08.2020).
29. Adamsky D. The Israeli Odyssey toward its National Cyber Security Strategy. *The Washington Quarterly*. 2017. Volume 40. Issue 2. P. 113–127. URL: <https://doi.org/10.1080/0163660X.2017.1328928>
30. Baezner M. Cybersecurity in Switzerland: Challenges and the Way Forward for the Swiss Armed Forces. *Connections. The Quarterly Journal*. Winter 2020. Vol. 19. No 1. URL: <http://connections-qj.org/article/cybersecurity-switzerland-challenges-and-way-forward-swiss-armed-forces> (Last Accessed: 20.08.2020).
31. Cohen M. S., Freilich Ch. D., Siboni G. Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives*, Volume 17, Issue 3, August 2016, Pages 307–321, <https://doi.org/10.1093/isp/ekv023>
32. 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-to-hide.html> (Last Accessed: 20.08.2020).
33. Şeker E., Tolga I. B. National Cyber Security Organisation: Turkey. Tallinn, 2018. 20 p.
34. 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/The-Privacy-Data-Protection-and-Cybersecurity-Law-Review-Edition-6-secured.pdf (Last Accessed: 20.08.2020).
35. Vozniuk E., Ukrainka L. Principles and Features of Japan's Information Security System. *Політичне життя*. 2017. № 4. С. 8–12.
36. What is the Difference between Cyber Security and Information Security? *Computer Science Degree Hub*. URL: <https://www.computersciencedegreehub.com/faq/what-is-the-difference-between-cyber-security-and-information-security/> (Last Accessed: 20.08.2020).
37. 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: 20.08.2020).

Допоміжна література

1. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України: 25.00.02 / Національна академія державного управління при Президентові України. Київ, 2017. 21 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: 23.00.03/ 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 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.
6. Власюк О. С. Національна безпека України: еволюція внутрішньої політики : вибрані наукові праці. Київ, 2016. 528 с.
7. 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: 20.08.2020).
8. Глобальна та національна безпека : підручник / авт. кол.: В. І. Абрамов., Г. П. Ситник, В. Ф. Смолянук ; за заг.ред. Г. П. Ситника. Київ: НАДУ, 2016. 784 с.
9. 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.
10. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Lviv Polytechnic National University Institutional Repository*. 2016. Vol. 2. No. 1. Р. 27–32. URL: http://ena.lp.edu.ua/bitstream/ntb/37314/1/7_31-36.pdf (дата звернення: 20.08.2020).
11. Корченко О. Г., Бурячок В. Л., С. О. Гнатюк. Кібернетична безпека держави: характерні ознаки та проблемні аспекти. *Безпека інформації*. 2013. Т. 19. № 1. С. 40–45.
12. 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.
13. Ліпкан В. А. Національна безпека України: навчальний посібник. Київ: КНТ, 2009. 576 с. URL: <http://politics.ellib.org.ua/pages-cat-154.html> (дата звернення: 20.08.2020).
14. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах Євроінтеграції: навчальний посібник. Серія: Національна і міжнародна безпека. Київ: КНТ, 2006. 280 с.
15. Малик Я. Інформаційна безпека України: стан та перспективи розвитку. *Ефективність державного управління*. 2015. Вип. 44. С. 13–20. URL: http://www.lvivacademy.com/vidavnistvo_1/edu_44/fail/ch_1/3.pdf (дата звернення: 20.08.2020).
16. Мануйлов Є. М., Ю. Ю. Калиновський. Роль і місце інформаційної безпеки держави у розбудові сучасної української держави. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого»*. 2016. № 2 (29). С. 144–153.

17. Мітін В. І. Інформаційний тероризм на сучасній міжнародній арені. *Международный научный журнал «Интернаука»*. 2017. № 2 (24). С. 65–68.
18. Негодченко В. Основні напрями державної інформаційної політики в Україні. *Підприємництво, господарство і право*. 2016. № 4. С. 77–81. URL: <http://pgp-journal.kiev.ua/archive/2016/04/15.pdf> (дата звернення: 20.08.2020).
19. Ничипорук Н., Вознюк Є. Секрет успіху США у сфері інформаційної безпеки. Міжнародні відносини, суспільні комунікації та регіональні студії. 2018. № 1 (3). С. 66–71.
20. Об информационном портале по безопасности. *SecurityLab.ru be Positive Technologies*. URL: <https://www.securitylab.ru/about.php> (Last Accessed: 20.08.2020).
21. Онкович А. Соцмережа Фейсбук та захист українського інформаційного простору в умовах російсько-українського конфлікту. *Український інформаційний простір*. 2020. Вип. 5. С. 233–242. URL: <http://ukrinfospace.knukim.edu.ua/article/view/206131/206151> (дата звернення: 20.08.2020).
22. Пилипчук В., Дзьобань О. Глобальні виклики й загрози національній безпеці держави в інформаційній сфері. *Вісник Національної академії правових наук України*. 2014. № 3 (78). С. 43–52.
23. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 20.08.2020).
24. 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.
25. 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.
26. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності. *Сучасний захист інформації*. 2016. № 4. С. 65–70.
27. Черновол І. Інформаційна безпека США в контексті актуальних загроз і викликів. Травневі студії 2020: історія, міжнародні відносини : збірник матеріалів Міжнародної наукової конференції «Травневі студії 2020: історія, міжнародні відносини» / за ред. Ю. Т. Темірова. Вінниця : Донецький національний університет імені Василя Стуса, 2020. Вип. 5. С. 67–69. URL: <http://jts.donnu.edu.ua/article/view/8277/8276> (дата звернення: 20.08.2020).
28. 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.
29. Collins A. *Contemporary Security Studies*. 3rd ed. United Kingdom: Oxford University Press, 2013. 478 p.
30. Isazadeh A. Information Society: Concepts and Definitions. *WSEAS Transactions on Systems*. January 2004. URL: https://www.researchgate.net/publication/254476368_Information_Society_Concepts_and_Definitions (Last Accessed: 20.08.2020).
31. Molander R. C., Riddle 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: 20.08.2020).
32. 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: 20.08.2020).

33. What is Information Security? URL: https://warwick.ac.uk/services/idc/informationsecurity/training/info_sec_quick_guide.pdf (Last Accessed: 20.08.2020).

Посилання на інформаційні ресурси в Інтернеті, відео-лекції, інше методичне забезпечення

1. Верховна Рада України - www.zakon1.rada.gov.ua.
2. Міністерство закордонних справ - <http://mfa.gov.ua/ua>
3. Міністерство юстиції - <https://minjust.gov.ua/ua>
4. Конституційний Суд України - <http://www.ccu.gov.ua/uk/index>
5. Організація Об'єднаних Націй - <http://www.un.org/>
6. Європейський суд з прав людини - <http://echr.coe.int/>
7. Європейський союз - <http://eeas.europa.eu/>
8. Організація з безпеки та співробітництва в Європі - <http://www.osce.org/>
9. Рада Європи - <http://www.coe.int/web/portal/home>
10. Управління Верховного комісара ООН з прав людини - <http://www.ohchr.org/>
11. Національна парламентська Бібліотека України - <http://www.nplu.org/>
12. Національна бібліотека України імені В. І. Вернадського - www.nbuv.gov.ua
13. Київська центральна міська публічна бібліотека ім. Лесі Українки - <http://lucl.lucl.kiev.ua>
14. Центральна наукова бібліотека Харківського національного університету ім. В.Н. Каразіна - <http://www.univer.kharkov.ua>
15. Харківська державна наукова бібліотека ім. В. Г. Короленка - <http://korolenko.kharkov.com>

11. Особливості навчання за денною формою в умовах продовження дії обставин непоборної сили (в тому числі запровадження карантинних обмежень через пандемію)

В умовах дії карантинних обмежень освітній процес в університеті здійснюється за змішаною формою навчання, а саме:

- дистанційно (за затвердженим розкладом занять) на платформі Zoom проводяться всі лекційні заняття;
- дистанційно на платформі Moodle проводяться семінарські, практичні, індивідуальні заняття та консультації, контроль самостійної роботи;
- аудиторно (за затвердженим розкладом занять) проводяться 10% практичних та семінарських занять у навчальних групах кількістю до 20 осіб з урахуванням відповідних санітарних і протиепідемічних заходів.

Складання підсумкового семестрового контролю: в разі запровадження жорстких карантинних обмежень з заборобою відвідування ЗВО здобувачам денної форми навчання надається можливість (за заявою, погодженою деканом факультету) скласти **залік дистанційно на платформі Moodle** <https://dist.karazin.ua/moodle/login/index.php>

12. Перелік питань до заліку

Заліковий білет містить 40 тестових завдань.

Питання для підготовки:

1. Основні положення Окінавської хартії глобального інформаційного суспільства від 22.07.2000 року: мета, основні положення.
2. Основні положення підсумкових документів Женевського етапу Всесвітнього саміту з питань інформаційного суспільства.

3. Основні положення підсумкових документів Туніського етапу Всесвітнього саміту з питань інформаційного суспільства.
4. Основні принципи інформаційного суспільства.
5. Типи і моделі побудови інформаційного суспільства.
6. Організаційно-правові основи розвитку інформаційного суспільства в Україні.
7. Завдання, цілі та напрями розвитку інформаційного суспільства в Україні.
8. Стратегія розвитку інформаційного суспільства в Україні: мета, принципи, завдання, етапи та основні напрями реалізації.
9. Поняття інформаційного простору та інформаційної сфери.
10. Структура та функції інформаційного простору.
11. Співвідношення понять «інформаційний простір» та «кіберпростір»
12. Поняття та основні характеристики національного інформаційного простору.
13. Мета формування і розвитку національного інформаційного простору України.
14. Підходи до визначення поняття «національна безпека держави».
15. Основні положення Закону України «Про національну безпеку України» від 21 червня 2018 року № 2469-VIII.
16. Поняття та сутність інформаційної безпеки держави.
17. Суб'єкти та механізми забезпечення інформаційної безпеки України.
18. Основні положення Закону України «Про інформацію» 1992 року;
19. Основні положення Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» 1994 року;
20. Основні положення Закону України «Про основні засади забезпечення кібербезпеки України» 2017 року;
21. Основні положення Указу Президента України № 287/2015 «Про рішення Ради національної безпеки і оборони України від 06 травня 2015 року «Про Стратегію національної безпеки України».
22. Основні положення Указу Президента України № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».
23. Основні положення Указу Президента України № 247/2017 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України».
24. Національні інтереси України в інформаційній сфері.
25. Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері.
26. Пріоритети державної політики в інформаційній сфері.
27. Роль Міністерства цифрової трансформації України у сфері захисту національного інформаційного простору України.
28. Роль Міністерства інформаційної політики України у сфері захисту національного інформаційного простору України.
29. 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.
30. Роль Служби безпеки України у сфері захисту національного інформаційного простору України.
31. Роль Департаменту кіберполіції Національної поліції України у сфері захисту національного інформаційного простору України.
32. Роль Державної служби спеціального зв'язку та захисту інформації України у сфері захисту національного інформаційного простору України.
33. Нормативно-правові інструменти захисту національного інформаційного простору США.

34. Інституційні інструменти захисту національного інформаційного простору США.

35. Особливості захисту національного інформаційного простору Великої Британії

36. Особливості захисту національного інформаційного простору Швейцарії.

37. Особливості захисту національного інформаційного простору країн ЄС.

38. Особливості захисту національного інформаційного простору Японії.

39. Особливості захисту національного інформаційного простору Китаю.

40. Особливості захисту національного інформаційного простору Ізраїлю.