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 ІЛЬЄНТЕЛЕЙМОНОВ

_____ 2020 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»

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___" _____08_____ 2020 року, протокол №__1__

РОЗРОБНИКИ ПРОГРАМИ: к.ю.н., доцент Сергій ЗДОРОВКО;
к.ю.н., Любомир ЗІНЯК

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

Протокол від "26__"___08_____2020 року № 1

Завідувач кафедри _____ Людмила НОВІКОВА
(підпис) (прізвище та ініціали)

Програму погоджено з гарантом освітньо-професійної програми

«Міжнародна інформаційна безпека»
назва освітньої програми

Гарант освітньо-професійної програми

«Міжнародна інформаційна безпека»
назва освітньої програми

_____ Людмила НОВІКОВА
(підпис)

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

Протокол від "28" 08 2020 року № 1

Голова науково- методичної комісії_____ Лариса ГРИГОРОВА-БЕРЕНДА
(підпис) (прізвище та ініціали)

ВСТУП

Програма навчальної дисципліни «Інформаційний тероризм» складена відповідно до освітньо-професійної програми підготовки **магістра** зі спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії», освітня програма «Міжнародна інформаційна безпека»

1. Опис навчальної дисципліни

1.1. Мета викладання навчальної дисципліни полягає у формуванні у здобувачів базових знань у сфері протидії інформаційному тероризму як загрози міжнародній та національній безпеці, а також практичних умінь та навичок правильного тлумачення та застосування механізмів інформаційної протидії, необхідних для їх майбутньої трудової діяльності як фахівців у сфері міжнародної інформаційної безпеки.

1.2. Основні завдання вивчення дисципліни:

- формування наступних загальних компетентностей:

ЗК7.Вміння аргументувати вибір шляхів вирішення завдань професійного характеру, критично оцінювати отримані результати та обгрунтовувати прийняті рішення.

ЗК11.Навички міжособистісної взаємодії, цінування та повага різноманітності та багатокультурності, здатність спілкування з представниками різних професійних груп різного рівня (з експертами з інших галузей знань/ видів діяльності)

- формування наступних фахових компетентностей:

ФК1. Поглилені знання про природу, динаміку, принципи організації міжнародних відносин, типи і види міжнародних акторів, сучасні тенденції світової політики.

ФК7. Здатність провадити прикладні аналітичні розробки проблем міжнародних відносин та світової політики, фахово готувати аналітичні матеріали та довідки.

ФК10

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	2-й
Семестр	
3-й	3-й
Лекції	
10 год.	год.
Практичні, семінарські заняття	

10 год.	год.
Лабораторні заняття	
Год	год.
Самостійна робота	
70 год	год.
Індивідуальні завдання	
Не передбачено	

1.6. Заплановані результати навчання:

Згідно з вимогами освітньо-професійної програми здобувачі мають досягти наступних результатів:

ПРН1. Фундаментальні знання щодо природи, джерел та напрямів еволюції міжнародних відносин, міжнародної політики, зовнішньої політики держав, стану теоретичних досліджень міжнародних відносин та світової політики.

ПРН4. Поглибленні знання проблем міжнародної та національної безпеки, міжнародних та інтернаціоналізованих конфліктів, підходів, способів та механізмів забезпечення безпеки у міжнародному просторі та у зовнішній політиці держав.

ПРН6. Демонструвати системне сприйняття та розуміння положень, які відносяться до галузі знань «Міжнародні відносини» або є складовою професійної практики.

ПРН11.Визначати та прогнозувати політичні, дипломатичні, безпекові, суспільні та інші ризики у сфері міжнародних відносин та глобального розвитку.

ПРН12.Оцінювати та аналізували міжнародні та зовнішньополітичні проблеми та ситуації, пропонувати підходи до вирішення таких проблем.

2. Тематичний план навчальної дисципліни

Розділ 1. Поняття інформаційного тероризму та способи протидії йому

Тема 1. Феномен інформаційного тероризму як загрози міжнародній та національній безпеці

Тероризм як явище. Закон України «Про боротьбу з тероризмом» від 20.03.2003 року. Поняття міжнародного тероризму. Складові терористичної дії (суб'єкт, об'єкт, причина і мотив, мета здійснення, часові та просторові характеристики. використовувані інструменти (засоби), наслідки). Поняття «інформаційний тероризм» та його характерні риси. Суб'єкти інформаційного тероризму. Характерні риси терористичних актів в інформаційній сфері. Види інформаційного тероризму (інформаційно-психологічний тероризм, інформаційно-технічний тероризм). Медіа-тероризм, його характерні риси та способи здійснення. Кібертероризм, його характерні риси, види та способи здійснення. Види правопорушень в інформаційній сфері (правопорушення проти цілісності та доступності комп'ютерних даних і систем: правопорушення, пов'язані з комп'ютерами; правопорушення, пов'язані зі змістом: правопорушення, пов'язані з порушенням авторських та суміжних прав).

Тема 2. Світовий досвід протидії інформаційному тероризму

Протидія інформаційному тероризму в рамках міжнародних організацій та форумів. Протидія інформаційному тероризму в рамках ООН. Глобальна контртерористична стратегія ООН

2006 року. Протидія інформаційному тероризму в рамках НАТО. Роль Інтерполу у протидії інформаційному тероризму. Угода між урядами держав-членів Шанхайської організації співробітництва про співробітництво у сфері забезпечення міжнародної інформаційної безпеки від 16.06.2009 року. Концептуальні підходи до питання інформаційного тероризму, що закріплені в концепції Конвенції про забезпечення міжнародної інформаційної безпеки, представленої у Лондоні у 2011 р. на Конференції з питань кіберпростору та у проекті «Загального договору з питань кібербезпеки та кіберзлочинності», так званому Договорі Шольберга. Періодизація превентивних заходів та контрзаходів світової спільноти у сфері протидії інформаційному тероризму. Механізми протидії інформаційному тероризму в США. Механізми протидії інформаційному тероризму в провідних державах Азії.

Тема 3. Механізми протидії інформаційному тероризму держав Європи

Засоби протидії інформаційному тероризму держав Європи на регіональному рівні. Поняття регіональної системи безпеки. Конвенція Ради Європи про кіберзлочинність від 23.11.2001 року. Роль ОБСЄ у протидії інформаційному тероризму держав Європи. Хартія європейської безпеки 1999 року. Рішення Ради Міністрів ОБСЄ № 3/04 «Боротьба з використанням Інтернету в терористичних цілях» 2004 року. Рішення Ради Міністрів ОБСЄ № 7/06 «Протидія використанню Інтернету в терористичних цілях» 2006 року. Протидія інформаційному тероризму в рамках ЄС. Ініціатива «Електронна Європа». Роль Агентства з мереж інформаційної безпеки (ENISA) у боротьбі з інформаційним тероризмом. Команда Реагування на Комп'ютерні надзвичайні події ЄС (CERT EU). Європейський центр по боротьбі з кіберзлочинністю (ЄС3). Стратегія кібербезпеки ЄС 2013 року. Директива 2016/1148 про заходи для забезпечення високого рівня безпеки мережевих та інформаційних систем у ЄС від 06.07.2016 року (NIS Directive). Роль Євроюсту та Європолу у протидії інформаційному тероризму у державах Європи. Засоби протидії інформаційному тероризму держав Європи на національному рівні. Досвід Естонії та Литви у боротьбі з інформаційним тероризмом. Особливості протидії інформаційному тероризму у Великій Британії, Німеччині, Бельгії, Франції та Іспанії Досвід протидії інформаційному тероризму у Туреччині.

Тема 4. Інформаційний тероризм як загроза національній безпеці України

Періодизація та види терористичних атак на інформаційний простір та кіберпростір України. Основні положення Законів України: «Про інформацію» від 2 жовтня 1992 року, «Про національну безпеку» від 21 червня 2018 року. «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року. «Про захист інформації в інформаційно-телекомунікаційних системах» від 5 липня 1994 року. Основні положення Указу Президента України від 25 лютого 2017 року «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Основні положення Указу Президента України від 15 березня 2016 року «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України ». Роль Служби безпеки України та Кіберполіції України у боротьбі з інформаційним тероризмом. Діяльність Команди реагування на комп'ютерні надзвичайні події в Україні (CERT-UA) у сфері протидії інформаційному тероризму. Діяльність Державного центру кіберзахисту та протидії кіберзагрозам (ДЦКЗ) в Україні у боротьбі з інформаційним тероризмом. Співробітництво України з міжнародними організаціями у сфері протидії інформаційному тероризму.

3. Структура навчальної дисципліни

Назва 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. Поняття інформаційного тероризму та способи протидії йому												
Тема 1. Феномен інформаційного тероризму як загрози міжнародній та національній безпеці.	19	2	2	-		15	-	-	-	-	-	-
Тема 2. Світовий досвід протидії інформаційному тероризму	19	2	2	-	-	15	-	-	-	-	-	-
Тема 3. Механізми протидії інформаційному тероризму держав Європи	29	4	4	-	-	25	-	-	-	-	-	-
Тема 4. Інформаційний тероризм як загроза національній безпеці України	19	2	2	-	-	15	-	-	-	-	-	-
Усього	90	10	10	-	-	70	-	-	-	-	-	-

4. Теми семінарських (практичних, лабораторних) занять

№ з/п	Назва теми	Кількість годин
1	Тема 1. Феномен інформаційного тероризму як загрози міжнародній та національній безпеці.	2
2	Тема 2. Світовий досвід протидії інформаційному тероризму.	2
3	Тема 3. Механізми протидії інформаційному тероризму держав Європи.	4
4	Тема 4. Інформаційний тероризм як загроза національній безпеці України.	2
	Разом	10

5. Завдання для самостійної роботи

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	**Феномен інформаційного тероризму як загрози міжнародній та національній безпеці**. *Завдання:* ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, розв'язати завдання за темою.	15
2	**Світовий досвід протидії інформаційному тероризму**. *Завдання:* ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, розв'язати завдання за темою.	15
3	**Механізми протидії інформаційному тероризму держав Європи**. *Завдання:* ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, розв'язати завдання за темою.	25
4	**Інформаційний тероризм як загроза національній безпеці України.** *Завдання:* ознайомитися з лекційним матеріалом та з матеріалами рекомендованої літератури за темою, підготувати інформаційні повідомлення та доповіді за питаннями теми семінарського заняття, відповісти на запитання для контролю знань, розв'язати завдання за темою.	15
	Разом	70

6. Індивідуальні завдання

Не передбачено.

7. Методи контролю

Поточний контроль знань здобувачів проводиться на кожному практичному (семінарському) аудиторному занятті у формі усного опитування, доповідей повідомлень здобувачів, розв'язання ситуативних та тестових завдань, навчальних дискусій, виконання творчих завдань. Сума балів за результатами роботи на практичних (семінарських) заняттях може сягати 60 балів.

Семестровий підсумковий контроль проводиться у формі заліку (максимальна сума балів - 40).

Підсумковий семестровий контроль здійснюється під час проведення екзамену. Загальна кількість балів за успішне виконання залікових завдань – 40. Час виконання – до 80 хвилин.

За бажанням здобувач має можливість обрати тестову форму залікоого білета (білет містить 20 тестових завдань, здобувач одержує 2 бали за кожну вірну відповідь)

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

У разі настання / подовження дії **обставин непоборної сили** (в тому числі запровадження жорстких карантинних обмежень в умовах пандемії з забороною відвідування ЗВО) здобувачам вищої освіти денної та заочної форм навчання надається можливість скласти **залік в тестовій формі** (білет містить 20 тестових завдань, здобувач одержує 2 бали за кожну вірну відповідь) **дистанційно на платформі Zoom** в дистанційному курсі «Інформаційний тероризм», режим доступу: https://us04web.zoom.us/j/6429687377?pwd=dGJxSXozZXQrUUJSbDViQXJlOGttdz09.

Схема нарахування балів

<table>
<tr><td colspan="4" rowspan="2">Поточний контроль, самостійна робота, індивідульні завдання</td><td></td><td colspan="2"></td></tr>
<tr><td>Разом</td><td>Залікова робота</td><td>Сума</td></tr>
<tr><td>Т1</td><td>Т2</td><td>Т3</td><td>Т4</td><td rowspan="2">60</td><td rowspan="2">40</td><td rowspan="2">100</td></tr>
<tr><td>16</td><td>14</td><td>18</td><td>12</td></tr>
<tr><td colspan="4">з якого - на практичних заняттях (бали)</td><td rowspan="4"></td><td rowspan="4"></td><td rowspan="4"></td></tr>
<tr><td>7</td><td>6</td><td>8</td><td>5</td></tr>
<tr><td colspan="4">з яких - самостійна робота здобувачів (бали)</td></tr>
<tr><td>9</td><td>8</td><td>10</td><td>7</td></tr>
</table>

Критерії оцінки успішності та результатів навчання

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

Розрахункова шкала для оцінювання роботи здобувачів на практичних (семінарських) заняттях:

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 обгрунтовані відповіді при виконанні завдань, здатність визначення теоретичних питань, на які розраховані завдання, уміння сформувати своє

	ставлення до певної проблеми теми, вміння мислити абстрактно й 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 обгрунтовані відповіді з несуттєвими помилками при виконанні завдань, здатність визначення теоретичних питань, на які розраховані завдання, уміння сформувати 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 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 шодо матеріалу тем змістовного розділу, неповні відповіді, допущення значної кількості помилок при виконанні 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, необгрунтовані 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, необгрунтовані відповіді, допущення істотних помилок при виконанні завдання, нездатність визначити теоретичні питання, на які розраховані завдання, невміння публічно представити матеріал.

Результати оцінювання роботи здобувачів фіксуються у відповідній відомості.

Здобувачі, знання яких оцінені мінімально необхідною для складання заліку кількістю балів, не мають право на виконання додаткових завдань для підвищення отриманої кількості балів.

Здобувачі, які були відсутні на лекції чи практичному (семінарському 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.

Підсумковий контроль знань здобувачів з навчальної дисциплін «Інформаційний тероризм» проводиться у формі заліку за 3-й семестр.

До заліку допускаються здобувачі, які були присутніми не менш ніж на 70% занять з навчальної дисципліни, враховуючи відпрацьовані. Основні питання зазначеної дисципліни містяться у залікових білетах. До кожного залікового білета включаються два теоретичних питання.

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

Кількість балів	**Критерії оцінювання**
35-40	Здобувач цілком і всебічно розкрив усі питання, вільно оперує поняттями і термінологією, демонструє глибокі знання джерел, має власну точку зору стосовно відповідних питань і може аргументовано її доводити.
29-34	Здобувач достатньо повно і всебічно розкрив усі питання, вільно оперує термінологією і поняттями, демонструє знання джерел, має власну точку зору стосовно відповідних питань і може аргументовано її доводити.
18-28	Здобувач розкрив питання у загальних рисах, але спостерігаються деякі упущення при відповіді на питання, обґрунтування неточні. Не підтверджуються достатньо обґрунтованими доказами.
10-17	Здобувач розкрив питання у загальних рисах, розуміє їхню сутність, намагається робити висновки, але при цьому слабко орієнтується в джерелах, припускається грубих помилок, матеріал викладає нелогічно.
0-9	Здобувач не в змозі дати відповідь на поставлені запитання, або відповідь не правильна, не розуміє суть питання. Не ознайомлений з джерелами. Не може зробити висновків.

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для дворівневої шкали оцінювання

90-100	зараховано
70-89	
50-69	
1-49	не зараховано

9. Рекомендована література

Основна література

1. Банк Р. О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект / Р. О. Банк. // Інформація і право. - 2016. – №1. - С. 110-116.

2. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок. В. Б. Толубко, В. О. Хорошко, В. О. Толюпа., 2015. - 288 с.

3. Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту : автореф. дис. на здобуття наук. ступеня канд. політ. наук : спец. 23.00.04 "Дипломатична академія України при МЗС України" / Валюшко І. О. - К., 2018. - 210 с.

4. Глазов О. В. Міжнародний інформаційний тероризм в контексті загроз національній безпеці України |Електронний ресурс) / 0. В. Глазов // Наукові праці. Політологія. – 2012. – Режим доступу до ресурсу: http://lib.chdu.edu.ua/pdf/naukpraci/politics/2012/197-185-15.pdf. (Дата звернення: 22.08.2019)

5. Гнатюк С. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи / С. Гнатюк. // Ukrainian Scientific Journal of Information Security. — 2013. — № 2.— С. 118-129.

6. Грицун О. О. Питання міжнародно-правового регулювання інформаційного тероризму. / О.О. Грицун // Часопис Київського університету права. 2014. № 4. С. 312 - 317.

7. Гуцалюк М. Кібертероризм та заходи протидії / М. Гуцалюк. // 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.

8. Давиденко М. О. Протидія СБ України терористичній пропаганді у інформаційному середовищі України / М. О. Давиденко. // 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. Режим доступу до ресурсу: http://academy.ssu.gov.ua/upload/file/konf_04_04_2019.pdf (Дата звернення: 22.08.2019).

9. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам / У. Ільницька. //Lviv Polytechnic National University Institutional Repository. — 2016. — № l. — С. 27-32. Режим доступу до ресурсу: http://ena.lp.edu.ua/bitstream/ntb/37314/1/7_31-36.pdf (Дата звернення: 20.08.2019).

10. Конвенція про кіберзлочинність: Міжнародний документ Ради Європи від 23 листопада |Електронний ресурс]. - 2001. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/994_575 (Дата звернення: 22.08.2019).

11. Крупнейшие кибератаки против Украины: с 2014 года. Инфографика. [Електронний ресурс] // Новое время. – 2017. – Режим доступу до ресурсу: https://nv.ua/ukraine/events/krupnejshie-kiberataki-protiv-ukrainy-s-2014-goda infografika-1438924. html. (Дата звернення: 24.05.2019).

12. Крупнейшие кибератаки против Украины: с 2014 года. Инфографика. [Електронний ресурс] // Новое время. – 2017. – Режим доступу до ресурсу: https://nv.ua/ukraine/events/krupnejshie-kiberataki-protiv-ukrainy-s-2014-goda infografika-1438924. html. (Дата звернення: 24.05.2019).

13. Малик Я. Інформаційна безпека України: стан та перспективи розвитку. / Я. Малик [Електронний ресурс] // Ефективність державного управління. 2015. Вип. 44. С. 13- 20. Режим доступу до ресурсу: http://www. lvivacademy.com/vidavnitstvo_1/edu_44/fail/ch_1/3.pdf (Дата звернення: 20.08.2019).

14. Мануйлов Є. М. Роль і місце інформаційної безпеки держави у розбудові сучасної української держави / Є. М. Мануйлов, Ю. Ю. Калиновський. // Вісник Національного університету «Юридична академія України імені Ярослава Мудрого». - 2016. - №2. - С. 144-153.

15. Матула М. Феномен інформаційного тероризму як загрози національній та міжнародній безпеці [Електронний ресурс] / М. Матула // Науковий блог. Національний університет «Острозька з академія». - 2014. – Режим доступу до ресурсу: https://naub.oa.edu.ua/2014/fenomen-informatsijnoho-teroryzmu-yak-zahrozy-natsionalnij-ta-mizhnarodnij-bezpetsi/ (Дата звернення: 22.08.2019).

16. Мітін В. І. Інформаційний тероризм на сучасній міжнародній арені / В.І. Мітін // Международный научньй журнал «Интернаука». 2017. № 2 (24). 1 т. С. 65-68.

17. Про боротьбу з тероризмом: Закон України від 20.03.2003 № 638-VI [Електронний ресурс] // Верховна Рада – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/638-15 (Дата звернення: 22.05.2019).

18. Про інформацію: Закон України від 02 жовтня 1992 № 2657-XII [Електронний ресуре] // Верховна | Рада України - Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12#n18 (Дата звернення: 20.08.2019).

19. Про Концепцію боротьби з тероризмом в Україні: Указ Президента України від 05 березня 2019 року № 53/2019. [Електронний ресуре] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/53/2019?lang=ru (Дата звернення: 20.08.2019).

20. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII [Електронний ресурсі] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2469-19 (Дата звернення: 20.08.2019).

21. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 року № 2163-VIII. [Електронний ресурсі] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2163-19 (Дата звернення: 20.08.2019).

22. 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 [Електронний ресурсі] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/287/2015 (Дата звернення: 20.08.2019).

23. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України: Указ Президента України від 15 березня 2016 року № 96/2016#n2 [Електронний ресуре] // Верховна Рада України - Режим доступу до ресурсу: : https://zakon.rada.gov.ua/laws/show/96/201 6#n2 (дата звернення: 22.08.2019).

24. 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. № 247/2017[Електронний ресурс] // Верховна Рада України – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/47/2017 (Дата звернення: 20.08.2019).

25. Руководство по передовой практике защиты важнейших обьектов неядерной

энергетической инфраструктуры: от террористических актов в связи є угрозами, исходящими из киберпространства (Електронний ресурс) // ОБСЕ. – 2013. – Режим доступу до ресурсу: https://www.osce.org/ru/secretariat/ 110472?download=true (Дата звернення: 22.08.2019).

26. Самые громкие кибер-атаки на критические инфраструктуры [Електронний ресурс] // Habr.. - 2016. – Режим доступу до ресурсу: https://habr.com/ru/company/panda/blog/3 16500/ (Дата звернення: 22.08.2019).

27. Семен Н. Ф. Російські Інтернет-ресурси як чинник інформаційної війни проти України (на прикладі сайтів «ПравдаРу» та «Российский диалог»): автореф. дис. на здобуття наук. ступеня канд. наук з соц. комун.: спец. 27.00.01 "Міжнародний економіко - гуманітарний університет імені акад. С. Демянчука; Дніпровьский національний університет імені Олеся Гончара" / Семен Н. Ф. - Рівне, 2018. - 250 с.

28. Ткачук Т. Інформаційна безпека держави в національному законодавстві європейських країн / Т. Ткачук [Електронний ресурс] // Visegrad Journal on Human Rights. — 2018 - №1. - С 145-150. — Режим доступу до ресурсу: http://vjhr.sk/archive/2018_1/part 2/24.pdf (Дата звернення: 20.08.2019).

29. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико правовий аналіз / Т. Ткачук [Електронний ресурсі] // Підприємництво, господарство і право. - 2017. - №10 - С. 182-186. – Режим доступу до ресурсу: : http://pgp-journal. kiev.ua/archive/2017/10/38.pdf (Дата звернення: 20.08.2019).

30. Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах Євроінтеграції України : дис. докт. юр. наук : 12.00.07 / Ткачук Т. Ю. ДВНЗ «Ужгородський національний університет. - Ужгород, 2019. - 487 с.

31. Форос А. В. Інформаційний тероризм як загроза національній безпеці України. /АВ. Форос // Правова держава. 2010. № 12. С. 256-261

32. Фролова 0. М. Роль ООН в системі міжнародної інформаційної безпеки. Міжнародні віносини [Електронний ресурс] / О. М. Фролова // Міжнародні віносини. Серія «Політичні науки». - 2018. - № 18-19. Режим доступу до ресурсу: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468 (Дата звернення : 22.08.2019).

33. Основні засоби інформаційного протиборства та інформаційної війни як явища сучасного міжнародного політичного процесу / І. М. Харченко, С. О. Сапогов, В. М. Шамраєва, Л. В. Новікова / Вісник Харківського національного університету імені В. Н. Кразіна. Серія «Міжнародні відносини. Економіка. Країнознавство. Туризм. - 2017. - №6. - С. 77-81. Режим доступу ресурсу: http://international-relations-tourism.karazin.ua/themes/irtb/resources/2c5d772b29 c5a9e2139a9f6aa96834d0.pdt (Дата звернення 20.08.2019).

34. Яцик Т. П. Особливості інформаційного тероризму як Одного із способів інформаційної війни. / Т. П. Яцик // Науковий вісник Національного університету ДПС України (економіка, право). 2014. № 2(65). С. 55-60.

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

36. Directive (Eu) 2016/1148 Of The European Parliament and Of The Council concerning measures for a high common level of security of network and information systems across the Union. [Електронний ресурс] // Official Journal of the European Union.. — 2016. — Режим доступу до ресурсу: https://eur-lex.europa.eu/eli/dir/2016/1148/oj} (Дата звернення: 22.05.2019).

37. European Commission. «eEurope - An information society for all» [Електронний ресурс] — Режим доступу до ресурсу: http://europa.eu/rapid/press-release_SPEECH-O1- 180_en.htm?locale=ru

(Дата звернення: 22.05.2019).

38. Global Cybersecurity Index (GCI) 2018 [Електронний ресурс] // Studies & Research. ITUPublications. — 2019. — Режим доступу до ресурсу: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf (Дата звернення: 22.08.2019).

39. Kumar M. European Union Parliament Under Cyber Attack! / M. Kumar // The Hacker News. March 29, 2011. URL: https://thehackernews.com/201 1/03/curopean-union- parliament-under-cyber.html (Дата звернення: 22.08.2019).

40. Lemos R. Cyberterrorism: The Real Risk. / R. Lemos // Computer Crime Research Center (CCRC). URL: http://www.crime%research.org/library/Robert|.htm (Дата звернення: 22.08.2019)

Допоміжна література

1. Антонюк В. В. Організаційно-правові засади формування та реалізації державної політики інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. держ. упр. : спец. 25.00.02 "Національна академія державного управління при Президентові України" / Антонюк В. В. - Київ, 2017. -21 с.

2. Возженников А. В. Международный терроризм: борьба за геополитическое господство. /А.В. Возженников Зксмо. Москва. 2007. 528 с.

3. Градов А. П. Деятельность Североатлантического союза в сфере кибербезопасности / А.П. Градов // Зарубежное военное обозрение. 2014. Вып. 7. С. 13-16.

4. Григорьев Н. Ю. Современный кибернетический терроризм и его социальные последствия / Н.Ю. Григорьев, З.Б. Родюков // Вестник университета. 2016. № 5. С. 227- 234.

5. Довгань О. Д. Кібертероризм як загроза інформаційному суверенітету держави / О.Д. Довгань, В.Г. Хлань // інформаційна безпека людини, суспільства, держави. № 3 (7). 2011. С. 49-53.

6. Журавель В. Противодействие угрозе кибертерроризма / В. Журавель // Зарубежное военное обозрение. 2018. №5. С. 12-15.

7. Корченко О. Г. Кібернетична безпека держави: характерні ознаки та проблемні аспекти / О.Г. Корченко, В.Л. Бурячок, С.О. Гнатюк // Безпека інформації. 2013. Т. 19. № 1. С. 40-45.

8. Лазарев Н. Я. Терроризм как социально-политическоє явление: истоки, формы и динамика развития в современных условиях : дис. канд. політ. наук : 23.00.01 / Лазарев Н. Я. - Москва, 2007. - 172 с.

9. Негодченко В. Основні напрями державної інформаційної політики в Україні / В. Негодченко В. [Електронний ресурсі]// Підприємництво, господарство і право. 2016. № 4. С. 77-81. Режим доступа до ресурса: http://pgp-journal.kiev.ua/archive/2016/04/15.pdf (дата зверненя: 20.08.2019).

10. Правовое регулирование борьбы с киберпреступностью, кибертерроризмом и трафиком людей: опыт Европейского союза / Отв. ред. В. Г. Киютин. А. І. Новиков. Бишкек-Москва, 2010. 239 с

11. Хмелевський Р. М. Дослідження оцінки загроз інформаційній безпеці об'єктів інформаційної діяльності / Р.М. Хмелевський // Сучасний захист інформації. 2016. № 4. С. 65-70.

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

13. Collins A. Contemporary Security Studies. 3rd ed. / A. Collins. — United Kingdom: Oxford

University Press, 2013. — 478 с.

14. ENISA. Cyber Europe 2018: After Action Report. 2018. Режим доступа до ресурса:https://www.enisa.europa.eu/publications/cyber-europe-2018-after-actionreport (Дата звернення:22.08.2019).

15. Petya Ransomware Outbreak: Here's What You Need To Know, Symantec Security Response. [Електронний ресурс] // Symantec. 24 October, 2017. Режим доступа до ресурсу: https://www.symantec,com/blogs/threat-intelligence/petya-ransomware-wiper (Дата звернення:22.08.2019).

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 - hitp://www.nplu.org/
12. Національна бібліотека України імені В. І. Вернадського - www.nbuy.gov.ua
13. Київська центральна міська публічна бібліотека ім. Лесі Українки - http://lucl.lucl.kiev.ua
14. Центральна наукова бібліотека Харківського національного університета ім. В. Н. Каразіна - http://www.univer.kharkov.ua
15. Харківська державна наукова бібліотека ім. В. Г. Короленка - http://korolenko.kharkov.com
16. European Union Agency For Cybersecurity (ENISA) — htt s://www.ecnisa.curopa.cu/
17. Computer Emergency Response Team of Ukraine (CERT-UA) — https://cert.gov.ua/
18. Офіційний сайт кіберполіції України — https://cyberpolice. gov.ua

10. Перелік питань до заліку

Заліковий білет містить 2 завдання, які полягають у розгорнутій відповіді на теоретичні питання курсу.

Питання для підготовки:

1. Складові терористичної дії.
2. Поняття «інформаційний тероризм» та його характерні риси.
3. Медіа-тероризм, його характерні риси та способи здійснення.
4. Кібертероризм, його характерні риси, види та способи здійснення. -
5. Види правопорушень в інформаційній сфері (правопорушення проти цілісності та доступності комп'ютерних даних і систем; правопорушення, пов'язані з комп'ютерами)
6. Види правопорушень в інформаційній сфері (правопорушення, пов'язані зі змістом; правопорушення, пов'язані з порушенням авторських та суміжних прав).

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

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

– дистанційно (за затвердженим розкладом занять) на платформі Zoom проводяться всі лекційні заняття;

– дистанційно на платформі Zoom https://us04web.zoom.us/j/6429687377?pwd=dGJxSXozZXQrUUJSbDViQXJlOGttdz09 проводяться практичні (семінарські), 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 забороною відвідування ЗВО здобувачам денної форми навчання надається можливість (за заявою, погодженою деканом факультету) скласти залік **в тестовій формі дистанційно на платформі Zoom** в дистанційному курсі «Інформаційний тероризм», режим доступу: https://us04web.zoom.us/j/6429687377?pwd=dGJxSXozZXQrUUJSbDViQXJlOGttdz09