Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут
«Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин

"ЗАТВЕРДЖУЮ"

Директор ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Микола ПИСАРЕВСЬКИЙ

«28» серпня 2025 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 безепка»
вид дисципліни за вибором
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»

2025 / 2026 навчальний рік

Програму рекомендовано до затвердження Вченою радою ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу

28 серпня 2025 року, протокол №1

РОЗРОБНИК ПРОГРАМИ:
Ірина ПАНОВА, канд. екон. наук, доцент, доцент кафедри міжнародних відносин

Програму схвалено на засіданні кафедри міжнародних відносин

Протокол від №1 від «25» серпня 2025 року

Завідувач кафедри _____ Наталія ВІННИКОВА
(підпис) (ім'я та прізвище)

Програму погоджено з гарантом освітньо-професійної програми «Міжнародні відносини»

Гарант освітньо-професійної програми
«Міжнародні відносини» (бакалаврського рівня)

_____ Наталія ВІННИКОВА
(підпис)

Програму погоджено науково-методичною комісією ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»

Протокол № 1 від «27» серпня 2025 року

Голова науково-методичної комісії _____ Ганна ПАНАСЕНКО
(підпис) (ім'я та прізвище)

ВСТУП

Програма навчальної дисципліни «Інформаційний тероризм » складена відповідно до освітньо-професійної (освітньо-наукової) програми підготовки

«Міжнародні інформаційна безпека»

рівень вищої освіти:другий (магістерський)

спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»

1. Опис навчальної дисципліни

1.1. Мета викладання 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

- сформувати розуміння сутності та характерних рис інформаційного тероризму, його видів і специфіки впливу на міжнародну та національну безпеку;
- проаналізувати світовий досвід протидії інформаційному тероризму на рівні міжнародних організацій (ООН, НАТО, ОБСЄ, ЄС) та провідних держав світу;
- ознайомити з механізмами і правовими інструментами протидії інформаційному тероризму в європейських країнах, а також із практиками національного рівня;
- дослідити загрози інформаційного тероризму для України, нормативно-правову базу та діяльність національних інституцій у сфері кібер- та інформаційної безпеки;
- розвинути здатність критично оцінювати сучасні інформаційні загрози й надавати практичні рекомендації щодо їх запобігання та нейтралізації на національному, регіональному і глобальному рівнях.

1.3. Кількість кредитів: 4

1.4. Загальна кількість годин: 120

1.5. Характеристика навчальної дисципліни	
За вибором	
Денна форма навчання	Заочна (дистанційна) форма навчання
Рік підготовки	
2-й	-
Семестр	
2-й	-
Лекції	
18 год.	-
Практичні, семінарські заняття	
4 год. (практ.), 5 год. (сем.)	-
Самостійна робота	
93 год.	-
у тому числі індивідуальні завдання	
-	-

1.6. Перелік компетентностей, що формує дана дисципліна

- формування наступних загальних компетентностей:

ЗК1. Здатність проводити дослідження на відповідному рівні.
ЗК3. Вміння виявляти, ставити та вирішувати проблеми.
ЗК5. Здатність генерувати нові ідеї (креативність).
ЗК6. Здатність працювати в міжнародному контексті.
ЗК7. Здатність працювати в команді.
ЗК9. Здатність оцінювати та забезпечувати якість виконуваних робіт.
ЗК10. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК11. Здатність планувати та управляти часом.
ЗК12. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

- формування наступних спеціальних компетентностей:

СК1. Здатність виявляти та аналізувати природу, динаміку, принципи організації міжнародних відносин, типи та види міжнародних акторів, сучасні тенденції розвитку світової політики.

СК2. Здатність приймати обґрунтовані рішення щодо здійснення міжнародної та зовнішньополітичної діяльності.

СК3. 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.

СК4. Здатність аналізувати глобальні процеси та їх вплив на міжнародні

та суспільні відносини, політичні та суспільні системи.

СК5. Здатність аналізувати та прогнозувати міжнародні відносини у різних контекстах, зокрема політичному, безпековому, правовому, економічному, суспільному, культурному та інформаційному.

СК7. Здатність здійснювати прикладні аналітичні дослідження проблем міжнародних відносин та світової політики, суспільних комунікацій, регіональних студій, професійно готувати аналітичні матеріали та довідки.

СК8. Здатність організовувати та проводити міжнародні зустрічі та переговори, розробляти, аналізувати і оцінювати дипломатичні та міжнародні документи.

СК9. Здатність виявляти та аналізувати особливості розвитку країн та регіонів, сучасних глобальних, регіональних та локальних процесів, та місця в них України.

СК10. Здатність до самонавчання, підтримки належного рівня знань, готовність до опанування знань нового рівня, підвищення своєї фаховості та рівня кваліфікації.

СК11. Здатність аналізувати природу та джерела зовнішньої політики, еволюцію підходів до її формування та здійснення, принципи організації системи зовнішньої політики та функціонування інститутів зовнішньої політики.

СК14. Здатність оцінювати зміст та основні напрями діяльності міжнародних організацій в сфері безпеки та сучасних стратегій забезпечення міжнародної інформаційної безпеки.

СК16. Здатність аналізувати основи та особливості захисту національного інформаційного простору та забезпечення інформаційної безпеки держави.

СК17. Здатність виявляти та аналізувати природу та специфічні особливості інформаційного тероризму.

1.7. Перелік результатів навчання, що формує дана дисципліна

Згідно з вимогами освітньо-професійної програми студенти повинні досягти наступних результатів:

РН2. Знати та розуміти сутність та специфічні особливості інформаційного протиборства та інформаційно-психологічних операцій в міжнародних відносинах.

РН3. Знати та розуміти основи та особливості захисту національного інформаційного простору та забезпечення інформаційної безпеки держави.

РН4. Знати та розуміти природу та специфічні особливості інформаційного тероризму.

1.8. Пререквізити

1. Актуальні проблеми міжнародних відносин та глобального розвитку
2. Політика європейської та євроатлантичної інтеграції
3. Міжнародне інформаційне право
4. Глобальна безпека та міжнародні конфлікти
5. Аналіз та прогнозування зовнішньої політики

2. Тематичний план навчальної дисципліни

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

Назви тем	Кількість годин					
	денна форма					
	усього	у тому числі				
		л	п	лаб.	інд.	с.р.
1	2	3	4	5	6	7
Тема 1. Феномен інформаційного тероризму як загрози міжнародній та національній безпеці	30	4	2/0			24
Тема 2. Світовий досвід протидії інформаційному тероризму	30	4	2/0			24
Тема 3. Механізми протидії інформаційному тероризму держав Європи	30	4	0/2			24
Тема 4. Інформаційний тероризм як загроза національній безпеці України	30	6	0/3			21
Усього годин	120	18	4/5			93

4. Теми семінарських (практичних, лабораторних) занять

№ з/п	Назва теми	Кількість годин
1	Тема 1. Феномен інформаційного тероризму як загрози міжнародній та національній безпеці	2/0
2	Тема 2. Світовий досвід протидії інформаційному тероризму	2/0
3	Тема 3. Механізми протидії інформаційному тероризму держав Європи	0/2
4	Тема 4. Інформаційний тероризм як загроза національній безпеці України	0/3
	Разом	4/5

5. Завдання для самостійної робота

№ з/п	Види, зміст самостійної роботи (доповіді)	Кількість годин
1	**Тема 1. Феномен інформаційного тероризму як загрози міжнародній та національній безпеці** ✓ Опрацювати наукові праці українських та зарубіжних дослідників (мін. 5 авторів) і узагальнити їх підходи до визначення понять «тероризм», «інформаційний тероризм». ✓ Скласти порівняльну таблицю видів інформаційного тероризму (інформаційно-психологічний, інформаційно-технічний, медіа-тероризм, кібертероризм) та їхніх характерних рис. ✓ Написати есе (до 3 стор.) на тему: «Інформаційний тероризм як новий вимір загроз глобальній та національній безпеці». ✓ Розробити схему «Суб'єкти інформаційного тероризму та їхні інструменти».	24
2	**Тема 2. Світовий досвід протидії інформаційному тероризму** ✓ Підготувати огляд міжнародних документів і стратегій (ООН, НАТО, ШОС, Конвенція про міжнародну інформаційну безпеку). ✓ Провести міні-дослідження (презентація 6–7 слайдів) про механізми протидії інформаційному тероризму в США, Китаї чи Японії. ✓ Скласти таблицю «Періодизація превентивних заходів і контрзаходів світової спільноти у сфері протидії інформаційному тероризму». ✓ Написати аналітичне повідомлення (до 3 стор.): «Які міжнародні механізми є найбільш ефективними у боротьбі з інформаційним тероризмом?».	24
3	**Тема 3. Механізми протидії інформаційному тероризму держав Європи** ✓ Опрацювати положення Конвенції Ради Європи про кіберзлочинність (2001 р.) та підготувати короткий огляд. ✓ Скласти таблицю «Інститути та інструменти ЄС у боротьбі з кіберзлочинністю та інформаційним тероризмом» (ENISA, CERT EU, ЄС3, Європол, Євроюст). ✓ Провести міні-дослідження (презентація 6–7 слайдів) про досвід однієї країни Європи (Естонія, Литва, Німеччина, Велика Британія, Франція). ✓ Написати есе (до 3 стор.): «Особливості європейського підходу до протидії інформаційному тероризму».	24
4	**Тема 4. Інформаційний тероризм як загроза національній безпеці України** ✓ Опрацювати закони та укази України у сфері кібер- та інформаційної безпеки («Про національну безпеку», «Про основні засади забезпечення кібербезпеки України», Доктрина інформаційної безпеки тощо). ✓ Скласти таблицю «Інституційна система протидії інформаційному тероризму в Україні» (СБУ, Кіберполіція, CERT-UA, ДЦКЗ). ✓ Провести міні-дослідження (презентація 6–7 слайдів) про приклади інформаційних атак проти України (2014–2024 рр.). ✓ Написати аналітичне повідомлення (до 3 стор.): «Міжнародне співробітництво України у сфері протидії інформаційному тероризму: здобутки та проблеми».	21
	Разом	93

6. Індивідуальні завдання

Не передбачені навчальним планом.

7. Методи навчання

У процесі навчання використовуються словесні методи: лекція, лекція-дискусія; наочні: наприклад, ділова гра; практичні: науково-дослідні завдання. Крім того, важливу роль відіграють творчі, проблемно-пошукові методи, пов'язані із постановкою наукової гіпотези, розгляд якої має знайти відображення в навчальній діяльності студентів.

8. Методи контролю

Система оцінювання знань, вмінь та навичок студентів передбачає виставлення оцінок за усіма формами проведення занять.

Перевірка та оцінювання знань студентів може проводитися у наступних формах:

- оцінювання роботи студентів під час практичних занять;
- оцінка за індивідуальну роботу студентів;
- проведення проміжного контролю;
- проведення підсумкового контролю.

Загальна оцінка з дисципліни визначається як сукупність балів, що студент отримує за змістовні модулі та модульний контроль. Проміжний контроль знань студентів здійснюється шляхом проведення тестування з основних навчальних елементів змістовних тем. Сума балів, які студент денної форми навчання може набрати за першим та другим розділом, дорівнює 60. Підсумковий контроль здійснюється у формі заліку. До заліку допускаються студенти, які мають достатню кількість балів з поточного контролю та написання і захисту індивідуальної роботи. Загальна кількість балів за успішне виконання залікових завдань становить 40.

Підсумковий контроль представлений у вигляді тестових питань. А саме – 40 тестових питань, кожне з яких важить 1 бал.

УВАГА! У разі використання заборонених джерел під час заліку студент на вимогу викладача залишає аудиторію та одержує загальну нульову оцінку (0). У разі настання / подовження дії обставин непоборної сили здобувачам вищої освіти денної форми навчання надається можливість скласти залік в тестовій формі (білет містить 20 тестових завдань, здобувач одержує 2 бали за кожну вірну відповідь) дистанційно на платформі Moodle в дистанційному курсі «Інформаційний тероризм».

Сумарна оцінка за вивчення дисципліни розраховується як сума

контрольних оцінок та балів, отриманих за результатами поточного та підсумкового семестрового контролю. Загальна сума балів підсумкового семестрового контролю складає 100.

9. Схема нарахування балів

Схема нарахування балів

Поточний контроль, самостійна робота					Проміжний контроль	Разом	Залікова робота	Сума
Т1	Т2	Т3	Т4	Т5	20	60	40	100
5	5	5	5	5				
60								

Т1, Т2 ... – теми розділів.

Структура та складові підсумкової оцінки з дисципліни

Поточний контроль протягом семестру – 60 балів. З них:

– активна робота на семінарських та практичних заняттях – 40 балів (5 балів кожна тема семінарського та практичного);

– ПК – 20 балів;

Поточний контроль проводиться на кожному семінарському занятті та за результатами виконання завдань самостійної роботи. Він передбачає оцінювання теоретичної підготовки здобувачів вищої освіти із зазначеної теми (у тому числі, самостійно опрацьованого матеріалу) під час роботи на семінарських заняттях.

Критерії поточного оцінювання знань студентів

Усний виступ, виконання письмового завдання	Критерії оцінювання
5	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу.
4	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки.
3	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки.

2	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхнево (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності.
1	Частково володіє навчальним матеріалом, не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки.
0	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань.

Доповнення виступу:

2 бали – отримують здобувачі вищої освіти, які глибоко володіють матеріалом, чітко визначили його зміст; зробили глибокий системний аналіз змісту виступу, виявили нові ідеї та положення, що не були розглянуті, але суттєво впливають на зміст доповіді, надали власні аргументи щодо основних положень даної теми.

1 бал отримують здобувачі, які виклали матеріал з обговорюваної теми, що доповнює зміст виступу, поглиблює знання з цієї теми та висловили власну думку.

Суттєві запитання до доповідачів:

2 бали отримують здобувачі вищої освіти, які своїм запитанням до виступаючого суттєво і конструктивно можуть доповнити хід обговорення теми.

1 бал отримують здобувачі вищої освіти, які у своєму запитанні до виступаючого вимагають додаткової інформації з ключових проблем теми, що розглядається.

Ведення опорного конспекту лекції:

Опорний конспект лекції (ОКЛ) – вид навчально-методичного посібника, в якому у стисло і системно викладено основний теоретичний матеріал у формі основних понять і положень, що структурно й логічно пов’язані між собою. Дані поняття та положення є лише опорними сигналами, вони вимагають пояснень і визначень, що мають записати студенти під час лекції. Його ведення сприяє системному і глибокому засвоєнню навчального матеріалу, дозволяє простежити структурні зв’язки між різними поняттями, положеннями, концепціями, проблемами, теоріями тощо.

Кожен студент повинен мати ОКЛ на лекціях і вести в ньому записи власноруч. Під час аудиторної роботи з ОКЛ студенти записують основні тези лекції та пояснення викладача у визначеному в конспекті полі. Під час самостійної роботи рекомендується доповнити записи лекції та завершити виконання завдань, що були зазначені в Робочій програмі та ОКЛ.

Критерії поточного контролю знань студентів

Поточний контроль проводиться з метою визначення стану успішності здобувачів вищої освіти за період теоретичного навчання. Поточний контроль знань студентів здійснюється через проведення аудиторних письмових контрольних робіт або комп'ютерного тестування. Зокрема, проведення двох таких робіт, кожна з яких важить 10 балів.

Письмова контрольна робота або тестування	Критерії оцінювання
10	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно розв'язав усі тестові завдання.
7-9	В цілому володіє навчальним матеріалом викладає його основний зміст під час письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно розв'язав половину тестових завдань.
4-6	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час письмових відповідей, недостатньо розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності, правильно розв'язав меншість тестових завдань.
1-3	В мінімальному обсязі володіє навчальним матеріалом. Дає відповідь лише на одне з двох теоретичних питань, при цьому недостатньо розкриває його зміст, а також допускає суттєві неточності. Правильно розв'язав декілька тестових завдань.
0	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.

Умови допуску здобувача до підсумкового семестрового контролю (заліку): виконання поточного контролю у вигляді тестів, роботи на семінарських та лекційних занять, за результатами яких він набрав не менше 10 балів.

Зарахування неформальної освіти та додаткових активностей

1. Зарахування сертифікованих курсів

Здобувачі вищої освіти можуть отримати додаткові бали за успішне проходження дистанційних курсів або тренінгів на провідних освітніх платформах (Coursera, Prometheus тощо), які тематично пов'язані зі змістом дисципліни.

Умови зарахування: студент має надати викладачеві офіційний документ (сертифікат або свідоцтво), що підтверджує успішне завершення курсу. Курс має бути погоджений з викладачем. Рекомендується обговорити вибір курсу заздалегідь. За успішне проходження одного курсу може бути зараховано до 5 балів додаткової поточної успішності.

2. Зарахування активної участі в наукових заходах

Додаткові бали можуть бути нараховані за активну участь у наукових конференціях, семінарах, публікацію наукових статей або тез досліджень.

Умови зарахування: студент має надати офіційне звернення до викладача. До звернення необхідно додати підтверджуючі документи (сертифікати учасника конференції, копії наукових публікацій, витяги з протоколів тощо).

Кількість балів: участь з доповіддю на науково-практичній конференції: до 5 балів; публікація тез конференції: до 5 балів; публікація статті у фаховому виданні: до 10 балів.

Кожне таке звернення розглядається окремо. Рішення ухвалюється відповідно до чинних нормативно-правових документів Харківського національного університету імені В. Н. Каразіна. Незалежно від кількості додаткових активностей, максимальний рівень поточної успішності не може перевищувати 60 балів.

У кінці семестру сумуються всі отримані студентом бали. Вказані вище види і форми засвоєння навчального курсу дають можливість набрати 60 балів та 40 балів за залікову роботу. Отже, максимальна кількість балів – 100.

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка
	для дворівневої шкали оцінювання
90 – 100	зараховано
70-89	
50-69	
0-49	не зараховано

10. Рекомендована література

Основна література

1. Захист прав, приватності та безпеки людини в інформаційну епоху / Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. – Київ-Одеса : Фенікс, 2020. 260 с. URL: https://ippi.org.ua/zakhist-pravprivatnosti-ta-bezpeki-lyudini-v-informatsiinu-epokhu

2. Інформаційно-комунікаційна безпека: сучасні тренди : моногр. / Бровко О. О. [та ін.] ; за заг. ред.: Курбан О. В., Лісневська А. Л. Київ : Київ. ун-т ім. Б. Грінченка, 2022.

3. . Інформаційне та соціально-правове моделювання: посібник / Д. В. Ланде, В. М. Фурашев; за заг. ред. Д. В. Ланде. Київ-Одеса : Фенікс, 2021. 276 с. URL: http://ippi.org.ua/sites/default/files/posibnik.pdf

4. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С.

Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І. Вернадського. URL: https://ippi.org.ua/kiberbezpeka-vinformatsiinomu-suspilstvi
5. Кібербезпека «суспільства знань»: монографія/ Довгань О., Тарасюк А., Ткачук Т. : монографія. Київ-Одеса : Фенікс, 2021. 176 с. URL: http://ippi.org.ua/kiberbezpeka- %C2%ABsuspilstva-znan%C2%BB
6. Когут Ю. І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології) : практич. посіб. Київ : Консалтингова компанія «СІДКОН»; ВД «Дакор», 2022. 284 с.
7. Мороз О. Як не стати овочем: інструкція з виживання в інфопросторі. Харків: Vivat, 2021. 256 с
8. Національна безпека: світоглядні та теоретико-методологічні засади: монографія / за заг. ред. О. П. Дзьобаня. Харків: Право, 2021. 776 с. URL: http://ippi.org.ua/natsionalna- bezpeka-svitoglyadni-ta-teoretiko-metodologichni-zasadi
9. Померанцев П. Це не пропаганда. Подорож на війну проти реальності : пер. з англ. Київ : Yakaboo Publishing, 2020. 288 с.
10. Правові засади забезпечення кібербезпеки в умовах цифрової трансформації: навчальний посібник / О. Довгань , Н. Ткачук , Т. Ткачук , В. Петров. – К., Артек. 2022. 171 с. URL: https://ippi.org.ua/pravovi-zasadi-zabezpechennya-kiberbezpeki-v-umovakh-tsifrovoitransformatsii
11. Права людини: інформаційний вимір: монографія / О.О. Тихомиров. – Одеса: Видавництво «Юридика», 2023. 304 с. URL: http://ippi.org.ua/sites/default/files/tihomirov_o.o._prava_lyudini_monografiya.pdf
12. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства: монографія / Н. Уханова; за заг. ред. В. Пилипчука. – Київ- Одеса: Фенікс, 2022. 140 с.
13. Соціальні та цифрові трансформації: нова парадигма кібербезпеки. Монографія. / О. А. Баранов. Київ: 2021. 86 с. URL: https://ippi.org.ua/sotsialni-ta-tsifrovi-transformatsiinova-paradigma-kiberbezpeki
14. Трансформація: соціальна & цифрова & правова: монографія у 3-х т. Т. 1. Порятунок цивілізації: економіка результату / О. А. Баранов. Одеса: Видавничий дім «Гельветика», 2022. 272 с. URL: https://ippi.org.ua/transformatsiya-sotsialna-tsifrova-pravova
15. Jetter, M. The effect of media attention on terrorism. *Journal of Public Economics*. 2017. 153, *32–48*. https://doi.org/10.1016/j.jpubeco.2017.07.006
16. Pitman L. On the scale from ransomware to cyberterrorism. *Journal of Cyber Policy*. 2024. https://doi.org/10.1080/23738871.2024.2377670
17. Schmid, A. P. Prevention of (ab-)use of mass media by terrorists. In *Handbook of Terrorism Prevention and Preparedness* (Chap. 18). The Hague: ICCT. 2020 https://icct.nl/sites/default/files/2023-01/Chapter-18-Handbook.pdf

Допоміжна література

1. Зражевська Н. І. Наративний рівень новин. Соціальні комунікації: теорія і практика сучасної науки: матеріали міжнар. наук.-практ. конф., 11–12 листопада 2022 р., Київ, 2022. С. 34–39. URL: http://catalog.lihapres.eu/index.php/liha-pres/catalog/book/169
2. Інформаційна війна: соціально-онтологічний та мілітарний аспекти : монографія / Р.В. Гула, О.П. Дзьобань, І.Г. Передерій, О.О. Павліченко, Г.О. Філь. Київ : «Каравела», 2020. 288 с.
3. Почепцов Г. Г. Токсичний інфопростір. Як зберегти ясність мислення і свободу дії. Харків: Vivat, 2021. 384 с
4. Саган О.В. Протидія медіаінформаційному тероризму як питання національної безпеки України : дис. ... канд. політ. наук : 21.01.01. Київ, 2021. 224 с

11. Посилання на інформаційні ресурси в Інтернеті, відеолекції, інше методичне забезпечення

1. Amnesty International. URL: https://www.amnesty.org.ua
2. Foreign Affairs /magazine/. URL: https://www.foreignaffairs.com
3. Foreign Policy. URL: https://foreignpolicy.com
4. International Security Journal. URL: https://direct.mit.edu/isec
5. UN News. Global perspective Human stories. https://news.un.org/en/
6. UN. URL: https://www.un.org/en/
7. Stockholm International Peace Research Institute. URL: https://sipri.org
8. RAND Corporation: Global Security. URL: https://www.rand.org/topics/global- security.html
9. The International Institute for Strategic Studies. URL: https://www.iiss.org
10. Закон України «Про національну безпеку України» (із змінами). URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
11. Про рішення Ради національної безпеки і оборони України від 25 березня 2021 року «Про Стратегію воєнної безпеки України». Указ Президента України №121/2021. URL: https://www.president.gov.ua/documents/1212021-37661

12. Особливості навчання за денною формою в умовах подовження дії обставин непоборної сили

В умовах дії **обставин непоборної сили** освітній процес в університеті здійснюється відповідно до наказів/ розпоряджень ректора/ проректора або за змішаною формою навчання або повністю дистанційно в синхронному

режимі.

Складання підсумкового семестрового контролю: в разі запровадження жорстких обмежень з забороною відвідування ЗВО студентам денної форми навчання надається можливість скласти залік дистанційно на платформі Moodle в дистанційному курсі «Інформаційний тероризм» https://moodle.karazin.ua/course/view.php?id=14786