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

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ЄС

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

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:
Віталій СОЛОВИХ, д.держ.упр., професор, професор кафедри міжнародних відносин

Програму схвалено на засіданні кафедри міжнародних відносин

Протокол №1 від «25» серпня 2025 року

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

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

Гарант освітньо-професійної програми
«Міжнародна інформаційна безпека» (магістерського рівня)

_____ Віталій СОЛОВИХ
(підпис) (ім'я та прізвище)

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 **«Стратегія кібербезпеки ЄС»** складена відповідно до освітньо-професійної програми **«Міжнародна інформаційна безпека»** підготовки **магістрів** за спеціальністю **291 «Міжнародні відносини, суспільні комунікації та регіональні студії»**

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1.1. Метою викладання навчальної дисципліни є формування у студентів системне уявлення про стратегічні засади, нормативно-правові основи, інституційну архітектуру та ключові напрямки реалізації політики кібербезпеки Європейського Союзу. Розвинути здатність критично аналізувати кіберзагрози, оцінювати ефективність заходів кіберстійкості, інтерпретувати міжнародний досвід забезпечення інформаційної безпеки та застосовувати отримані знання для розробки національних підходів у сфері цифрової безпеки в міжнародному контексті.

1.2. Основні завдання вивчення дисципліни

1. Сформувати здатність до аналізу політики кібербезпеки ЄС у контексті глобальних безпекових викликів і тенденцій цифрової трансформації.
2. Ознайомити з правовими основами кібербезпеки ЄС, зокрема нормативними актами (NIS2, Cyber Resilience Act, DORA), та навчити аналізувати їхній вплив на державну та корпоративну безпеку.
3. Розвинути здатність ідентифікувати актуальні кіберзагрози та гібридні виклики, пов’язані з діяльністю державних та недержавних акторів, зокрема в умовах війни та політичної дестабілізації.
4. Сприяти формуванню навичок критичного осмислення діяльності міжнародних організацій у сфері кібербезпеки, включаючи ENISA, Європейську Комісію, НАТО та інші.
5. Навчити оцінювати стратегії кіберстійкості, зокрема заходи щодо захисту критичної інфраструктури, підготовки кадрів, управління ризиками та реагування на інциденти.
6. Формувати практичні навички порівняльного аналізу кіберполітик ЄС та України, з урахуванням інституційного, стратегічного та правового контекстів.

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	-й
Семестр	
3-й	-й
Лекції	
18 год.	год.
Практичні, семінарські заняття	
4/5 год.	год.
Лабораторні заняття	
- год.	год.
Самостійна робота	
93 год	год.
Індивідуальні завдання	
-	

1.6. Перелік компетентностей, що формує дисципліна

Загальні компетентності (ЗК):

ЗК1. Здатність проводити дослідження на відповідному рівні.

ЗК3. Вміння виявляти, ставити та вирішувати проблеми.

ЗК6. Здатність працювати в міжнародному контексті.

Фахові (спеціальні) компетентності (СК):

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… безпековому, правовому, економічному тощо.

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.

1.7. Заплановані результати навчання

У результаті вивчення даного курсу здобувач повинен

РН5. Критично осмислювати та аналізувати глобальні процеси та їх вплив на міжнародні відносини.

РН7. Аналізувати та оцінювати проблеми міжнародної та національної безпеки, механізми забезпечення безпеки у міжнародному просторі.

РН16. Аналізувати та оцінювати сучасні стратегії забезпечення міжнародної інформаційної безпеки.

РН17. Аналізувати та оцінювати зміст та специфіку основних напрямів діяльності міжнародних організацій в сфері безпеки.

1.8. Пререквізити (дисципліни, що передують вивченню)

Для успішного засвоєння дисципліни **«Стратегія кібербезпеки ЄС»** студенти мають оволодіти знаннями та навичками, здобутими під час вивчення таких навчальних дисциплін: Політика європейської та євроатлантичної інтеграції, Міжнародне інформаційне право, Глобальна безпека та міжнародні конфлікти, Міжнародна інформаційна безпека

2. ТЕМАТИЧНИЙ ПЛАН НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Основи стратегії кібербезпеки ЄС

Поняття кібербезпеки в контексті ЄС. Роль цифрової європейської політики. Мета та принципи стратегії кібербезпеки ЄС. Роль ENISA (Агентство з кібербезпеки ЄС). Співвідношення між стратегією кібербезпеки ЄС та національними стратегіями.

Тема 2. Європейська правова база кібербезпеки

Загальні рамки правового регулювання. Директива NIS2: зміст і значення. Акт про кіберстійкість (Cyber Resilience Act). Співвідношення норм ЄС з національним законодавством. Санкційна політика ЄС проти кіберзагроз.

Тема 3. Інституції ЄС у сфері кібербезпеки

Європейська Комісія та її функції в кібербезпеці. Агентство ENISA: роль та повноваження. Роль Європейської Ради та Ради ЄС. Співпраця з НАТО. Взаємодія з приватним сектором.

Тема 4. Загрози кібербезпеки для ЄС

Основні види сучасних кіберзагроз. Гібридні загрози: характер та особливості. Вплив державних акторів (напр. РФ, КНР). Інциденти в інфраструктурі ЄС. Психологічні операції та кібервійна.

Тема 5. Спільна політика безпеки та оборони (CSDP) в кіберсфері

CSDP та її компоненти. Роль кіберкоманд в оборонній політиці ЄС. Військово-цивільна взаємодія. Вправи та симуляції кібервійни. Співпраця з НАТО та ООН.

Тема 6. Кібердипломатія Європейського Союзу

Що таке кібердипломатія? Санкційні механізми проти кіберзлочинців.

Угода про цифрову співпрацю (EU–US). Діалог ЄС–ООН про кібербезпеку. Цифрові права людини.

Тема 7. Співпраця ЄС з Україною у сфері кібербезпеки

Політичні рамки кіберспівпраці. Підтримка України з боку ЄС (після 2022). Синхронізація стратегій. Захист критичної інфраструктури. Перспективи членства в цифровому союзі.

Тема 8. Стратегія кіберстійкості: впровадження на практиці

Що таке кіберстійкість? Ідентифікація вразливостей. Практики бізнес-континуїті. Навчання та підготовка кадрів. Оцінка ефективності кіберзахисту.

Тема 9. Перспективи розвитку кібербезпеки в ЄС до 2030 року

Кіберзагрози майбутнього. Роль ШІ та автоматизації. Цифрова

автономія ЄС. Розвиток кіберосвіти та кадрів. Нові ініціативи: DORA, AI Act тощо.

3. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Назви розділів і тем	Кількість годин					
	Денна форма					
	Усього	У тому числі				
		л	п/с	лаб	інд	с.р
1	2	3	4	5	6	7
Тема 1. Основи стратегії кібербезпеки ЄС	13	2	0/1			10
Тема 2. Європейська правова база кібербезпеки	13	2	0/1			10
Тема 3. Інституції ЄС у сфері кібербезпеки	13	2	0/1			10
Тема 4. Загрози кібербезпеки для ЄС	13	2	0/1			10
Тема 5. Спільна політика безпеки та оборони (CSDP) в кіберсфері	13	2	0/1			10
Тема 6. Кібердипломатія Європейського Союзу	13	2	1/0			10
Тема 7. Співпраця ЄС з Україною у сфері кібербезпеки	14	2	1/0			11
Тема 8. Стратегія кіберстійкості: впровадження на практиці	14	2	1/0			11
Тема 9. Перспективи розвитку кібербезпеки в ЄС до 2030 року	14	2	1/0			11
Разом	120	18	4/5			93

4. Теми семінарських (практичних, лабораторних) занять

4.1. Теми семінарських занять

№ з/п	Назва теми	Кількість годин
1	Тема 1. Основи стратегії кібербезпеки ЄС	1
	Тема 2. Європейська правова база кібербезпеки	1
2	Тема 3. Інституції ЄС у сфері кібербезпеки	1
	Тема 4. Загрози кібербезпеки для ЄС	1
3	Тема 5. Спільна політика безпеки та оборони (CSDP) в кіберсфері	1
	Разом	5

4.2. Теми практичних занять

№ з/п	Назва теми	Кількість годин
1	Тема 6. Кібердипломатія Європейського Союзу	1
	Тема 7. Співпраця ЄС з Україною у сфері кібербезпеки	1
2	Тема 8. Стратегія кіберстійкості: впровадження на практиці	1
	Тема 9. Перспективи розвитку кібербезпеки в ЄС до 2030 року	1
	Разом	4

5. САМОСТІЙНА РОБОТА СТУДЕНТІВ

№ з/п	Види, зміст самостійної роботи	Кількість годин
1	**Тема 1. Основи стратегії кібербезпеки ЄС** 1. Опишіть основні принципи та цілі стратегії кібербезпеки ЄС. Наведіть приклади їх реалізації у політиці безпеки. 2. Знайдіть офіційний документ «EU Cybersecurity Strategy for the Digital Decade» (2020/2023) і зробіть короткий конспект його ключових положень. 3. Порівняйте поняття «кібербезпека» у стратегії ЄС та українському законодавстві. Визначте спільні риси та відмінності.	10
2	**Тема 2. Європейська правова база кібербезпеки** 1. Проаналізуйте основні положення директиви NIS2. Поясніть, які категорії суб'єктів вона охоплює. 2. Складіть таблицю, що порівнює директиву NIS2 і Акт про кіберстійкість (CRA) за такими критеріями: об'єкт регулювання, відповідальність, впровадження. 3. Підготуйте огляд санкційного механізму ЄС у сфері кібербезпеки, наведіть приклади його застосування.	10
3	**Тема 3. Інституції ЄС у сфері кібербезпеки** 1. Складіть схему взаємодії основних європейських інституцій (Єврокомісія, ENISA, Рада ЄС) у сфері кібербезпеки. 2. Підготуйте коротке досьє про агентство ENISA: його функції, інструменти, ключові ініціативи. 3. Дослідіть роль приватного сектору в реалізації стратегії ЄС. Наведіть приклади публічно-приватного партнерства.	10

4	**Тема 4. Загрози кібербезпеки для ЄС** 1. Знайдіть і проаналізуйте останній звіт ENISA щодо кіберзагроз. Випишіть 3 ключові загрози з коротким описом. 2. Наведіть приклади гібридних загроз для ЄС (особливо після 2022 року). Проаналізуйте інструменти протидії. 3. Підготуйте таблицю типових кіберінцидентів останніх років в ЄС: дата, країна, характер атаки, наслідки.	10
5	**Тема 5. CSDP та кіберсфера** 1. Розкрийте поняття CSDP (Спільна політика безпеки і оборони ЄС) та її зв'язок з кібербезпекою. 2. Опишіть приклад навчань або симуляцій з кібероборони в межах CSDP/NATO. 3. Складіть короткий аналітичний огляд політики ЄС щодо оборони кіберпростору у 2022–2024 роках.	10
6	**Тема 6. Кібердипломатія ЄС** 1. Дослідіть, що таке «EU Cyber Diplomacy Toolbox». Коротко опишіть його зміст та функції. 2. Наведіть приклади застосування санкцій ЄС за участь у кібератаках. Які країни потрапляли під них? 3. Напишіть коротке есе на тему: «Цифрові права людини як інструмент кібердипломатії ЄС».	10
7	**Тема 7. Співпраця ЄС з Україною** 1. Дослідіть проєкти, у яких ЄС підтримує кібербезпеку України. Коротко опишіть хоча б два приклади. 2. Підготуйте порівняльну таблицю стратегічних документів з кібербезпеки України та ЄС. 3. Визначте перспективи участі України в європейських програмах кіберзахисту (Digital Europe, NIS тощо).	11
8	**Тема 8. Стратегія кіберстійкості** 1. Опишіть етапи впровадження системи кіберстійкості у підприємствах критичної інфраструктури. 2. Розробіть базовий план реагування на кіберінцидент для організації. 3. Знайдіть приклади використання кіберстійкості у практиці країн ЄС (навести 1–2 кейси).	11
9	**Тема 9. Перспективи кібербезпеки ЄС до 2030 року** 1. Прогнозуйте основні загрози, які, на думку фахівців ЄС, можуть з'явитися до 2030 року. 2. Проаналізуйте положення DORA та AI Act щодо майбутньої кібербезпеки.	11

	3. Напишіть есе на тему: «Якою має бути стратегія кібербезпеки ЄС у 2030-х роках?».	
	Разом	93

6. ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Індивідуальне завдання, відповідно до навчального плану, не передбачене.

7. МЕТОДИ НАВЧАННЯ

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

Таблиця 7.1

Методи навчання та засоби діагностики результатів навчання за освітньою компонентною

Шифр ПРН (відповідно до ОПП)	Результати навчання (відповідно до ОПП)	Методи навчання	Засоби діагностики /форми оцінювання
РН05	Критично осмислювати та аналізувати глобальні процеси та їх вплив на міжнародні відносини.	Лекція; пошук джерел інформації (критичний аналіз, інтерпретація), корегування та підготовка частини наукового дослідження, її презентація	Оцінювання усних відповідей на практичних заняттях, оцінювання аналітичної частини дослідження, залікова робота
РН07	Аналізувати та оцінювати проблеми міжнародної та національної безпеки, механізми забезпечення безпеки у міжнародному просторі.	Лекція; пошук джерел інформації (критичний аналіз, інтерпретація), корегування та підготовка частини наукового дослідження, її презентація	Оцінювання усних відповідей на практичних заняттях, оцінювання аналітичної частини дослідження, залікова робота

РН016	Аналізувати та оцінювати сучасні стратегії забезпечення міжнародної інформаційної безпеки.	Лекція; пошук джерел інформації (критичний аналіз, інтерпретація), корегування та підготовка частини наукового дослідження, її презентація	Оцінювання усних відповідей на практичних заняттях, оцінювання аналітичної частини дослідження, залікова робота
РН17.	Володіти навичками професійного усного та письмового перекладу з/на іноземні мови, зокрема, з фахової тематики міжнародного співробітництва, зовнішньої політики, міжнародних комунікацій, регіональних студій, дво- та багатосторонніх міжнародних проектів.	Лекція; пошук джерел інформації (критичний аналіз, інтерпретація), корегування та підготовка частини наукового дослідження, її презентація	Оцінювання усних відповідей на практичних заняттях, оцінювання аналітичної частини дослідження, залікова робота

8. МЕТОДИ КОНТРОЛЮ

При вивченні дисципліни застосовуються наступні методи контролю: усний, письмовий та тестовий. Контроль з дисципліни складається з поточного контролю, який проводиться у формі усного опитування або письмового експрес-контролю на лекціях, у формі виступів здобувачів при обговоренні питань на проблемних лекціях, у формі тестування, тощо, а також підготовки курсової роботи у вигляді проекту. Результати поточного контролю (поточна успішність) є основною інформацією для визначення модульної оцінки, при проведенні заліку і враховуються при визначенні підсумкової залікової оцінки з дисципліни.

Засвоєння тем (поточний контроль) контролюється на підсумкових заняттях та/або виконанням індивідуальної роботи

Застосовуються такі засоби діагностики рівня підготовки здобувачів:

- тестові завдання;

- виконання творчих завдань;

Поточний контроль є складовою системи організації навчального процесу. Завданням поточного контролю є оцінювання знань, умінь та практичних навичок здобувачів, набутих під час засвоєння дисципліни.

Поточний контроль здійснюється під час проведення практичних та семінарських занять, підсумкового контролю за підсумками вивчення дисципліни. Сума балів, які здобувач денної форми навчання може набрати за поточним контролями, дорівнює 60.

Підсумковий контроль засвоєння розділів здійснюється по їх завершенню на підсумкових заняттях.

Оцінка успішності здобувача з дисципліни є рейтинговою і виставляється за багатобальною шкалою з урахуванням оцінок засвоєння окремих розділів.

Підсумковий семестровий контроль здійснюється під час проведення заліку в 3 семестрі. Загальна кількість балів за успішне виконання залікових завдань – 40.

9. СХЕМА НАРАХУВАННЯ БАЛІВ

		Поточний контроль, самостійна робота, індивідуальні завдання								Зал робота	Сума
									Разом		
Т.1	Т.2	Т.3	Т.4	Т.5	Т.6	Т.7	Т.8	Т.9	60	40	100
6	6	6	7	7	7	7	7	7			

Критерії поточного оцінювання знань студентів

Усний виступ та виконання письмового завдання (реферат, есе, презентація)	**Критерії оцінювання**
5	Студент у повному обсязі володіє навчальним матеріалом, вільно, самостійно та аргументовано викладає його у процесі усних виступів і письмових відповідей. Демонструє глибоке та всебічне розуміння змісту теоретичних питань і практичних завдань, використовуючи при цьому як обов'язкову, так і додаткову літературу. Правильно вирішив усі тестові завдання.
4	Студент достатньо повно володіє навчальним матеріалом, обґрунтовано викладає його під час усних виступів та письмових відповідей. У основному розкриває зміст теоретичних питань і практичних завдань, використовуючи при цьому обов'язкову літературу. Проте під час викладу окремих питань не завжди досягає достатньої глибини та аргументованості; допускаються окремі несуттєві неточності й незначні помилки. Правильно вирішив більшість тестових завдань.
3	Студент у цілому володіє навчальним матеріалом,

	відтворює його основний зміст під час усних виступів та письмових відповідей, проте без глибокого та всебічного аналізу, обґрунтування й аргументації. Не завжди використовує необхідну літературу. При цьому допускаються окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
2	Студент не в повному обсязі володіє навчальним матеріалом, подає його фрагментарно й поверхово, без належної аргументації та обґрунтування під час усних виступів і письмових відповідей. Недостатньо розкриває зміст теоретичних питань та практичних завдань. При цьому допускає суттєві неточності. Правильно вирішив меншість тестових завдань.
1	Студент частково володіє навчальним матеріалом, не в змозі викласти зміст більшості питань під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив лише окремі тестові завдання.

Поточне оцінювання з дисципліни

№ з/п	Загальна (максимальна) кількість балів	Складові до загальної кількості балів	Вид роботи
Тема 1	6	5	виступ на семінарському/практичному занятті / доповідь або підготовка презентації за темою
		1	виконання завдань самостійної роботи
Тема 2	6	5	виступ на семінарському/практичному занятті / доповідь або підготовка презентації за темою
		1	виконання завдань самостійної роботи
Тема 3	6	5	виступ на семінарському/практичному занятті / доповідь або підготовка презентації за темою
		1	виконання завдань самостійної роботи

№ з/п	Загальна (максимальна) кількість балів	Складові до загальної кількості балів	Вид роботи
Тема 4	7	5	виступ на семінарському/практичному занятті / доповідь або підготовка презентації за темою
		2	виконання завдань самостійної роботи
Тема 5	7	5	виступ на семінарському/практичному занятті / доповідь або підготовка презентації за темою
		2	виконання завдань самостійної роботи
Тема 6	7	5	виступ на семінарському/практичному занятті / доповідь або підготовка презентації за темою
		2	виконання завдань самостійної роботи
Тема 7	7	5	виступ на семінарському/практичному занятті / доповідь або підготовка презентації за темою
		2	виконання завдань самостійної роботи
Тема 8	7	5	виступ на семінарському/практичному занятті / доповідь або підготовка презентації за темою
		2	виконання завдань самостійної роботи
Тема 9	7	5	виступ на семінарському/практичному занятті / доповідь або підготовка

№ з/п	Загальна (максимальна) кількість балів	Складові до загальної кількості балів	Вид роботи
			презентації за темою
		2	виконання завдань самостійної роботи
Усього	60		

Для допуску до семестрового контролю необхідно набрати не менше 30 балів за поточну діяльність.

Семестровий підсумковий контроль з дисципліни є обов'язковою формою контролю навчальних досягнень здобувача. Він проводиться відповідно до навчального плану у вигляді семестрового заліку в терміни, встановлені графіком навчального процесу та в обсязі навчального матеріалу, визначеному цією робочою програмою дисципліни.

Підсумковий семестровий контроль

Підсумковий семестровий контроль проводиться у формі заліку.

Загальна кількість балів за успішне виконання завдань – **40 балів**.

Час на виконання – **до 80 хвилин**.

Вміст залікового білета та система оцінювання:

- Теоретичне питання 1 – 20 балів
- Тести – 20 балів (10 тестових завдань × 2 бали)

Оцінювання теоретичного питання (1 питання 20 балів)

- 16–20 балів – здобувач вищої освіти в повному обсязі володіє навчальним матеріалом, грамотно, вільно та аргументовано його викладає; наводить визначення основних понять; глибоко та всебічно розкриває зміст поставленого питання; правильно інтерпретує основні принципи і положення; демонструє розуміння етапів розвитку міжнародної інформації; виявляє знання основної і додаткової літератури з дисципліни.
- 11–15 балів – здобувач вищої освіти в достатньому обсязі володіє навчальним матеріалом, вільно та грамотно його викладає, проте подекуди недостатньо аргументовано; розкриває зміст поставленого питання, використовуючи лише обов'язкову літературу; демонструє загальне розуміння суті дисципліни та значення інформації у системі наукового знання.
- 6–10 балів – здобувач вищої освіти загалом володіє навчальним матеріалом, однак не демонструє цілісності засвоєних знань; відповідь має неузгоджений характер, наявні невідповідності щодо основного понятійно-категоріального апарату дисципліни; допускаються граматичні помилки; відсутнє розуміння специфічності інформаційного потоку.
- 1–5 балів – здобувач вищої освіти володіє матеріалом фрагментарно й поверхнево; недостатньо розкриває зміст поставлених питань;

демонструє непослідовне трактування етапів становлення та розвитку міжнародної інформації; плутається в об'єкті та предметі дослідження; не володіє термінологією; не знає видатних персоналій; демонструє низьку грамотність.

За бажанням здобувач має можливість обрати тестову форму залікового 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).

Сумарна оцінка за вивчення дисципліни розраховується як сума модульних оцінок та балів, отриманих за результатами підсумкового семестрового контролю. Загальна сума балів модульних і підсумкового семестрового контролю складає 100.

Замість виконання завдань (вивчення тем) можуть також додатково враховуватись такі види активностей здобувача:

– проходження тренінг-курсів чи дистанційних курсів з використання сучасних освітніх технологій на платформах Coursera, Prometheus тощо (за наявності відповідного документу про їх закінчення, надання копії викладачу);

– участь в майстер-класах, форумах, конференціях, семінарах, зустрічах з проблем використання сучасних освітніх технологій (з підготовкою есе, прес-релізу, інформаційного повідомлення тощо, що підтверджено навчальною програмою заходу чи відповідним сертифікатом);

– участь у науково-дослідних та прикладних дослідженнях з проблем використання сучасних освітніх технологій (в розробці анкетних форм, проведенні опитувань, підготовці та проведенні фокус-груп, обробці результатів дослідження, підготовці звіту, презентації результатів тощо, що підтверджується демонстрацією відповідних матеріалів).

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

1. Грінченко О. В. Інституційні основи кіберстратегії ЄС. Безпекознавство. 2022. № 3. С. 56–62.
2. Куценко І. В. Європейське кіберзаконодавство: виклики для України. Право і кібербезпека. 2022. № 1. С. 12–20.
3. Мельник П. В. Політика кібербезпеки в Європейському Союзі: сучасні тренди. Наука і безпека. 2024. № 1. С. 41–48.
4. Пащенко С. М. Агентство ENISA: функції та завдання. Інформаційна безпека. 2023. № 3.
5. Тимошенко С. Кіберстійкість критичних систем. Безпекові технології. 2022.
6. Шестак З. О. Стратегія ЄС у сфері кібербезпеки: виклики та перспективи. Інформаційна безпека України. 2023. № 2. С. 15–25.
7. European Commission. The EU's Cybersecurity Strategy for the Digital Decade. 2023.
8. European Commission. Roadmap to 2030 – Cybersecurity in the Digital Decade. 2023.
9. European Union Agency for Cybersecurity (ENISA). Annual Report 2024.
10. Shah I. H. Digital Operational Resilience Act (DORA)... SSRN. 2025.

Допоміжна література

1. Білоус Ю. ЄС 2030: стратегічні напрями кібербезпеки. Політика та майбутнє. 2024.
2. Бондар О. П. Євроінтеграційна взаємодія у сфері кібербезпеки. Кіберпростір і право. 2024. № 1.
3. Василенко Д. І. Кібердипломатія ЄС. Міжнародні відносини та безпека. 2022.
4. Гусєв О. В. ЄС і НАТО в протидії кіберзагрозам. Україна і світ. 2024.
5. Дубров Д. В. Кіберконфлікти в Європі: аналіз випадків. Геополітика і безпека. 2022.
6. Кірєєв В. Співробітництво Україна–ЄС у цифровій сфері. Дипломатичний огляд. 2023.
7. Коноваленко А. М. Директива NIS2 та її впровадження в країнах-членах ЄС. Юридичний вісник Європи. 2023. № 4. С. 30–37.
8. Корнієнко М. Ю. Гібридна війна і кібербезпека. Безпека і суспільство. 2024.
9. Литвин І. Кіберпростір майбутнього: тренди. ІТ і держава. 2023.
10. Литвиненко С. І. Воєнна безпека в цифрову епоху. Оборонна стратегія. 2023.
11. Мірошниченко В. Кібераудит у практиці ЄС. Інформаційна політика. 2024.

12. Орлова І. Кіберсанкції як інструмент впливу. Європейське право. 2023.
13. Панченко Л. В. Кібербезпека в рамках CSDP. Європейські студії. 2022.
14. Сидоренко І. Кіберінтеграція України. Україна–ЄС. 2022.
15. Стрижак О. В. Глобальна цифрова дипломатія. Цифрове суспільство. 2024.
16. Хоменко Л. Кібертренінги в ЄС: методики та підходи. Освіта і безпека. 2023.
17. Хомутенко В. С. Кіберрегіоналізм в ЄС. Інформаційне право України. 2024.
18. Черниш Т. А. Сучасні кіберзагрози для ЄС. Інформаційна політика. 2023. № 4.
19. Шпак Р. Синхронізація політик у сфері кібербезпеки. Аналітика і прогнози. 2024.
20. Яременко В. І. Інституційна структура кібербезпеки в ЄС. Українська безпекова політика. 2022. № 2.
21. Appachikumar A. Open Banking and Consumer Privacy... IJIRP. 2025.
22. Birge L. Europeanizing Cybersecurity... 2025.
23. Chorna V., Bohdan B. Development of Cybersecurity of Critical Infrastructure... 2025.
24. Cotroneo C., Stolz M., Costantino F. Addressing Cyber-Attacks Against Critical Infrastructures... 2025.
25. EU Cyber Diplomacy Toolbox. European Council. 2024.
26. European External Action Service. EU Cyber Defence Policy Framework. 2023.
27. Honcharuk V., Karpenko M. Legal Regulation of National Security in Ukraine... 2025.
28. Kotal A. Cybersecurity: Applying Threat Modeling... SAE. 2025.
29. Krajewski K., Frąckiewicz D. Russian Influence Operations... Defence Science Review. 2025.
30. Leontić M. Smart Cities... European Safety Engineer. 2025.
31. Pandolfo L. A Knowledge-Driven Approach to Threat Validation... IEEE. 2025.
32. Perälä P., Lehto M. Advancing Cybersecurity Education... JYU. 2025.
33. Shah I. H. Empirical Analysis of DORA and Global ICT Frameworks. SSRN. 2025.

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

1. Cybersecurity Strategy for the Digital Decade URL:https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
2. Publications – European Union Agency for Cybersecurity (ENISA) URL:https://www.enisa.europa.eu/publications

3. Digital Operational Resilience Act (DORA) – European Commission URL:https://finance.ec.europa.eu/regulation-and-supervision/digital-finance/digital-operational-resilience_en

4. Міністерство цифрової трансформації України. Офіційний вебсайт URL:https://thedigital.gov.ua

5. Національний координаційний центр кібербезпеки при РНБО України. Офіційний вебсайт URL:https://ncscc.gov.ua

6. Національний інститут стратегічних досліджень. Співпраця України та ЄС у сфері кібербезпеки URL:https://niss.gov.ua/doslidzhennya/mizhnarodna-bezpeka/spivpratsya-ukrayiny-ta-yes-u-sferi-kiberbezpeky

7. Cybersecurity Policy Explained – Webinar by European Commission URL:https://www.youtube.com/watch?v=rEzPVZZ1ZUE

8. Prometheus. Курс «Кібербезпека та інформаційна війна» URL:https://prometheus.org.ua/course/cybersecurity/

9. EU CyberNet Academy. Introduction to EU Cybersecurity Policy URL:https://academy.eucybernet.eu

10. EU Law and Digital Resilience – Open Access Repository URL:https://op.europa.eu/en/publication-detail/-/publication/4ac8d77a-7dcd-11ec-9136-01aa75ed71a1/language-en

12. ОСОБЛИВОСТІ НАВЧАННЯ ЗА ДЕННОЮ ФОРМОЮ В УМОВАХ ПОДОВЖЕННЯ ДІЇ ОБСТАВИН НЕПОБОРНОЇ СИЛИ

В умовах дії **обставин непереборної 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 «Стратегія кібербезпеки ЄС».