МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Волинський національний університет імені Лесі Українки
Факультет міжнародних відносин
Кафедра міжнародних комунікацій та політичного аналізу

СИЛАБУС
нормативного освітнього компонента
ІНФОРМАЦІЙНА ПОЛІТИКА І БЕЗПЕКА

підготовки Бакалавра
спеціальності 291 Міжнародні відносини, суспільні комунікації та регіональні студії
освітньо-професійної програми Міжнародна інформація та суспільні комунікації

Луцьк – 2022

Силабус освітнього компонента «Інформаційна політика і безпека**»** підготовки бакалавра, галузі знань 29 Міжнародні відносини, спеціальності 291 Міжнародні відносини, суспільні комунікації та регіональні студії, за освітньою програмою Міжнародна інформація та суспільні комунікації.

Розробник: Федонюк Сергій Валентинович, доцент кафедри міжнародних комунікацій та політичного аналізу, кандидат географічних наук, доцент.

Погоджено
Гарант освітньо-професійної програми:
Федонюк С. В.

Силабус освітнього компонента затверджено на засіданні кафедри
Міжнародних комунікацій та політичного аналізу

протокол № 1 від 29 серпня 2022 р.

Завідувач кафедри: Карпчук Н. П.

І. Опис освітнього компонента

<table>
<tr><th>Найменування показників</th><th>Галузь знань, спеціальність, освітньо-професійна /освітньо-наукова/освітньо-творча програма, освітній рівень</th><th>Характеристика освітнього компонента</th></tr>
<tr><td rowspan="2">Денна форма навчання</td><td rowspan="6">Галузь знань:
“Міжнародні відносини”
Спеціалність:
291 Міжнародні відносини, суспільні комунікації та регіональні студії
Освітньо-професійна програма:
Міжнародна інформація та суспільні комунікації
Освітній рівень: Бакалавр</td><td>Нормативний</td></tr>
<tr><td>Рік навчання 1</td></tr>
<tr><td rowspan="2">Кількість годин/кредитів
150/5</td><td>Семестр 1-ий</td></tr>
<tr><td>Лекції 26 год.</td></tr>
<tr><td rowspan="2">ІНДЗ: немає</td><td>Семінарські 30 год.
Лабораторні ____ год.
Індивідуальні _____ год.</td></tr>
<tr><td>Самостійна робота 84 год.</td></tr>
<tr><td colspan="2">Мова навчання</td><td>українська</td></tr>
</table>

ІІ. Інформація про викладача

ПІП - Федонюк Сергій Валентинович
Науковий ступінь - кандидат географічних наук
Вчене звання - доцент
Посада - доцент кафедри міжнародних комунікацій та політичного аналізу
Контактна інформація sergii.fedoniuk@vnu.edu.ua.
Дні занять: заняття проводяться відповідно до розкладу занять,
який розміщений на сайті http://94.130.69.82/cgi-bin/timetable.cgi

ІІІ. Опис освітнього компонента

1. Анотація курсу

Курс «Інформаційна політика і безпека» призначений для знайомства студентів з політологічними і нормативними підходами, сучасними тенденціями в оцінці значення інформаційної політики та проблеми інформаційної безпеки в міжнародному політичному процесі. Дає змогу визначити місце, особливості та основні тенденції трансформації глобальної безпеки в зв'язку із загальною інформатизацією, революцією у військовій справі і формуванням інформаційного суспільства, а також впливом цих тенденцій на зовнішню політику України та інших держав.

2. **Пререквізити** (*попередні курси, на яких базується вивчення освітнього компонента*).

Цей курс вивчається у першому семестрі й не вимагає попереднього завершення освоєння визначених освітньо-професійною програмою освітніх компонентів.

Постреквізити (*освітні компоненти, для вивчення яких потрібні знання, уміння і навички, що здобуваються після закінчення вивчення даного освітнього компонента).*

Цей курс є базовим для наступного формування компетентностей у сфері інформаційної безпеки, зокрема в рамках таких освітніх компонентів: Стратегічні комунікації в міжнародних відносинах; Стратегії миру та міжнародної безпеки.

3. Мета і завдання освітнього компонента

Метою курсу формування відповідних компетентностей у фахівців, здатних розв’язувати складні спеціалізовані задачі та практичні проблеми професійної діяльності у сфері міжнародних відносин та зовнішньої політики, пов’язаній з інформаційною політикою та інформаційною (кібер) безпекою.

Курс орієнтований на формування: знань про місце інформаційної політики й безпеки в світових політичних процесах, логіку змін і розвитку проблеми інформаційної безпеки; вміння визначати характер загроз, пов'язаних з процесами інформатизації й розвитку кіберпростору; навички аналізу основних концептуальних підходів у інформаційній політиці та забезпечення інформаційної безпеки, а також вміння аналізу конкретних подій у сфері безпеки в зв'язку реалізацією положень документів стратегічного планування головних міжнародних акторів у сфері інформаційної (кібер) безпеки, динамікою процесів у сфері міжнародної безпеки.

4. **Результати навчання (компетентності)**

У переліку програмних компетентностей і результатів навчання (https://volnu-my.sharepoint.com/:w:/g/personal/sergii_fedoniuk_vnu_edu_ua/ESAULb4HSL5KrZIWPa6YlQMBFvBR-iNDNdn4KXCLjIPS3w?e=tutjay) цей освітній компонент забезпечує такі:

ЗК1. Здатність реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина України;
ЗК2. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі і знань про природу і суспільство, та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового образу життя.
ЗК4. Знання та розуміння предметної області та розуміння професійної діяльності.
ЗК5. Здатність працювати в міжнародному контексті.
ЗК6. Здатність генерувати нові ідеї (креативність).
ЗК7. Здатність застосовувати знання у практичних ситуаціях.
ЗК8. Здатність до абстрактного мислення, аналізу та синтезу.
ЗК9. Здатність використовувати інформаційні та комунікаційні технології.
ЗК10. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК12. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК13. Здатність бути критичним і самокритичним.
СК1. Здатність виокремлювати ознаки та тенденції розвитку, розуміти природу, динаміку, принципи організації міжнародних відносин, суспільних комунікацій та/або регіональних студій.
СК2.Здатність аналізувати міжнародні процеси у різних контекстах, зокрема політичному, безпековому, правовому, економічному, суспільному, культурному та інформаційному.
СК3. Здатність оцінювати стан та напрями досліджень міжнародних відносин та світової політики у політичній, економічній, юридичній науках, у міждисциплінарних дослідженнях.
СК4. Здатність розв'язувати складні спеціалізовані задачі і практичні проблеми у сфері міжнародних відносин, зовнішньої політики держав, суспільних комунікацій, регіональних досліджень.
СК5. Здатність аналізувати вплив світової економіки, міжнародного права та внутрішньої політики на структуру й динаміку міжнародних відносин та зовнішньої політики держав.
СК7. Здатність аналізувати міжнародні інтеграційні процеси у світі та на Європейському континенті, та місце в них України.
СК8. Усвідомлення національних інтересів України на міжнародній арені.
СК9. Здатність застосовувати знання характеристик розвитку країн та регіонів, особливостей та закономірностей глобальних процесів та місця в них окремих держав для розв'язання складних спеціалізованих задач і проблем.
СК11. Здатність аналізувати природу та еволюцію міжнародних організацій, їх місця у системі міжнародних відносин, основних форм та перспектив співпраці України з ними.
СК13. Здатність аналізувати діяльність міжнародних недержавних акторів та транснаціональні відносини.
РН01. Знати та розуміти природу міжнародних відносин та регіонального розвитку, еволюцію, стан теоретичних досліджень міжнародних відносин та світової політики, а також природу та джерела політики держав на міжнародній арені і діяльності інших учасників міжнародних відносин.
РН02. Знати та розуміти природу та динаміку міжнародної безпеки, розуміти особливості її забезпечення на глобальному, регіональному та національному рівні, знати природу та підходи до вирішення міжнародних та інтернаціоналізованих конфліктів.
РН03. Знати природу міжнародного співробітництва, характер взаємодії між міжнародним акторами, співвідношення державних, недержавних акторів у світовій політиці.
РН04. Знати принципи, механізми та процеси забезпечення зовнішньої політики держав, взаємодії між зовнішньою та внутрішньою політикою, визначення та реалізації на міжнародній арені національних інтересів держав, процесу формування та реалізації зовнішньополітичних рішень.
РН05. Знати природу та механізми міжнародних комунікацій.

РН06. Знати природу та характер взаємодій окремих країн та регіонів на глобальному, регіональному та локальному рівнях.
РН07. Здійснювати опис та аналіз міжнародної ситуації, збирати з різних джерел необхідну для цього інформацію про міжнародні та зовнішньополітичні події та процеси.
РН08. Збирати, обробляти та аналізувати великі обсяги інформації про стан міжнародних відносин, зовнішньої політики України та інших держав, регіональних систем, міжнародних комунікацій.
РН09. Досліджувати проблеми міжнародних відносин, регіонального розвитку, зовнішньої політики, міжнародних комунікацій, із використанням сучасних політичних, економічних і правових теорій та концепцій, наукових методів та міждисциплінарних підходів, презентувати результати досліджень, надавати відповідні рекомендації.
РН10. Вільно спілкуватися державною та іноземними мовами на професійному рівні, необхідному для ведення професійної дискусії, підготовки аналітичних та дослідницьких документів.
РН11. Здійснювати прикладний аналіз міжнародних відносин, зовнішньої політики України та інших держав, міжнародних процесів та міжнародної ситуації відповідно до поставлених цілей, готувати інформаційні та аналітичні.
РН13. Вести фахову дискусію із проблем міжнародних відносин, міжнародних комунікацій, регіональних студій, зовнішньої політичної діяльності, аргументувати свою позицію, поважати опонентів і їхню точки зору.
РН14. Використовувати сучасні цифрові технології, спеціалізовані програмне забезпечення, бази даних та інформаційні системи для розв’язання складних спеціалізованих задач у сфері міжнародних відносин, суспільних комунікацій та/або регіональних студій.
РН15. Розуміти та застосовувати для розв’язання складних спеціалізованих задач міжнародних відносин, суспільних комунікацій та регіональних студій чинне законодавство, міжнародні нормативні документи і угоди, довідкові матеріали, чинні стандарти і технічні умови тощо.
РН16. Розуміти та відстоювати національні інтереси України у міжнародній діяльності.
РН17. Мати навички самостійного визначення освітніх цілей та навчання, пошуку необхідних для їх досягнення освітніх ресурсів.

5. Структура освітнього компонента.

Тема	**Предмет вивчення**	**Усього***	**Лк ***	**Семін ***	**Самост.***	**Консуль***	**Форма контр., бал**
Змістовий модуль 1. Інформаційна політика та безпека в міжнародних відносинах							
1.1 Інформаційна політика та безпека: підходи і концепції	Інформаційна політика. Цілі інформаційної політики. Інформаційна політика держав. Координація міжнародної інформаційної політики. Виклики і загрози безпеки в інформаційну епоху. Інформаційно-технічні та соціо-гуманітарні аспекти інформаційної безпеки. Інформаційний простір і кібер-простір. Інформаційна безпека і кібер-безпека: порівняльний аналіз дослідницьких дискурсів та політичної практики. Національні підходи до визначення інформаційної безпеки. Діяльність міжнародних організацій у сфері інформаційної політики. Офіційні документи міжнародних організацій. Суб'єкти інформаційного впливу - держави і недержавні гравці.	8	4	4	10	1	ДС, 4
1.2 Об'єкти інформаційної безпеки	Об'єкти безпеки в інформаційну епоху. Інформаційні системи. Критична інформаційна інфраструктура. Визначення критичних інформаційних інфраструктур в різних країнах.	4	2	2	8	1	ДС/Р, 4

	Специфіка інформаційних інфраструктур з точки зору забезпечення їх безпеки. Виклики і загрози національній і міжнародній безпеці, пов'язані з впливом на критичні інформаційні інфраструктури. Роль бізнесу.						
1.3 Інформаційний тероризм і інформаційна злочинність.	Інформаційний тероризм і трансформація міжнародного тероризму. Використання інтернету в злочинних цілях. Комерційний потенціал інформаційної злочинності. Міжнародно-політичний вимір проблем інформаційного тероризму та інформаційної злочинності.	4	2	2	8	1	ДС/Р, 4
1.4 Ініціативи в галузі інформаційної безпеки	Позиція США і країн Заходу. Позиція Росії. Розстановка сил на світовій арені у зв'язку з російськими та американськими ініціативами у сфері інформаційної/кібер-безпеки. Позиція Китаю. Позиція Європейського Союзу. Позиція України.	8	4	4	10	1	ДС
1.5 Переговорний процес і міжнародне співробітництво в галузі забезпечення інформаційної безпеки.	Робота Комітетів ООН з безпеки і роззброєння, космосу, МСЕ, G7, Регіональних організацій. Позиції й інтереси провідних акторів у сфері міжнародної інформаційної безпеки та управління інтернетом. Співвідношення регіонального та глобального рівня міжнародної взаємодії щодо забезпечення інформаційної безпеки. Досвід міжнародного співробітництв в інших високотехнологічних областях світової політики (космос, контроль над ядерними озброєннями) і його придатність до інформаційної сфери.	6	2	4	8	1	ДС/РМГ,4
1.6 Міжнародне право в аспекті інформаційної безпеки.	Застосування загальних принципів міжнародного права до боротьби в інформаційній сфері. Міжнародне право збройних конфліктів і його придатність до дій в інформаційній сфері. Міжнародне гуманітарне право і його придатність до конфліктів із застосуванням інформаційних засобів. “Талліннське керівництво про можливість застосування міжнародного права до ведення кібер-воєн”. Національні підходи в питанні застосування права міжнародних конфліктів до інформаційної сфери. Застосування міжнародного договірного права в галузі роззброєння до питання обмеження інформаційного зброї. Основні напрями адаптації	8	4	4	10	1	ДС/РМГ, 5

	міжнародного права до інформаційної сфери.						
Разом за модулем 1		38	18	20	54	6	24
Змістовий модуль 2. Інформаційна політика та безпека України							
2.1. Основи інформаційної політики та безпеки України	Національна інформаційна політика України. Основні національні інтереси України в інформаційній сфері. Основні засади інформаційної безпеки України. Інформаційна безпека в системі забезпечення національної безпеки України. Напрями державної політики у сфері інформаційної безпеки України. Стратегія інформаційної безпеки України.	4	2	2	10	2	ДС, 5
2.2. Реалізація інформаційної політики та безпеки в Україні	Інституційно-правова основа інформаційної політики Нормативно-правова база. Діяльність органів державної влади загальної компетенції. Діяльність органів спеціальної компетенції. Діяльність громадських об'єднань та публічних інституцій у сфері інформаційної політики.	6	2	4	10	1	ДС, 5
2.3. Діяльність України на міжнародній арені у сфері інформаційної політики та безпеки	Інформаційна політика та безпека в аспекті функціонування системи зовнішньої політики України. Інституційна основа та організація. Позиція України з актуальних питань інформаційної політики та безпеки. Взаємодія з міжнародними організаціями. Співпраця у сфері інформаційної політики та безпеки з іноземними державами та Європейським Союзом.	8	4	4	10	1	ДС, 5
Разом за модулем 2		18	8	10	30	4	15
Всього годин/Балів		56	26	30	84	10	40

Методи контролю*: ДС – дискусія, ДБ – дебати, Т – тести, ТР – тренінг, РЗ/К – розв'язування задач/кейсів, ІНДЗ/ІРС – індивідуальне завдання/індивідуальна робота здобувача освіти, РМГ – робота в малих групах, МКР/КР – модульна контрольна робота/ контрольна робота, Р – реферат, а також аналітична записка, аналітичне есе, аналіз твору тощо.

6. Завдання для самостійного опрацювання.

Підготувати аналітичну довідку на одну із вказаних тем (або на додатково узгоджену тему)

1. Місце проблеми забезпечення інформаційної безпеки в сучасній світовій політиці.
2. Істинність і помилковість тези: «Хто володіє інформацією той володіє світом».
3. Зміна поняття «безпека» в інформаційному суспільстві.
4. Теоретичні підходи до аналізу логіки інформаційної війни і забезпечення військово-політичної безпеки.
5. Основні чинники, що визначають нові параметри проблеми забезпечення інформаційної безпеки.
6. Зміна характеру і пріоритетності загроз інформаційної безпеки в міжнародному аспекті.
7. Співвідношення завдань забезпечення національної і інформаційної безпеки.
8. Проблема міжнародного інформаційного тероризму.
9. Зміна парадигм тероризму в інформаційному суспільстві.
10. Проблема правового регулювання конфліктів із застосуванням інформаційних засобів дії.
11. Проблема війни і миру в інформаційному суспільстві.
12. Аналіз одного з сучасних конфліктів із позицій інформаційного протиборства.

13. Проблема розповсюдження інформаційної зброї.
14. Проблема контролю над інформаційними озброєннями.
15. Зміна характеру і пріоритетності загроз безпеки в інформаційному суспільстві.
16. Співпраця і розбіжності в підходах у сфері забезпечення інформаційної безпеки між Україною і США.

Питання для самостійного опрацювання
1. Де витоки кіберзагроз?
2. Чому одні дослідники вивчають інформаційну безпеку, а інші - кібербезпеку?
3. Які є наукові підходи до проблеми управління інтернетом?
4. Які основні підходи до проблеми інформаційної безпеки з точки зору міжнародного права?
5. Як по-різному розглядають інформаційні загрози військового характеру представники країн Заходу та Росії?
6. Яких позицій щодо проблем інформаційної безпеки дотримуються українські науковці?
7. Як сучасні ринкові процеси і розвиток інтернету впливають виникнення потенційних кібер-загроз?
8. Про що свідчить зростання витрат на кібербезпеку?
9. У чому проявляються новітні кіберзагрози?
10. Що таке "кіберзлочинність"?
11. Чи можуть кібернападники мати політичні цілі? Чи відомі Вам кібератаки такого виду"
12. Що таке "кібертероризм"? У чому полягають відмінності трактування цього поняття?
13. Які є прояви кібертероризму?
14. Які є види інформаційних воєнного характеру?
15. У чому сіть основних позицій держав із приводу міжнародно-правового регулювання інформаційної (кібер) безпеки?
16. Чи інформація й програмне забезпечення можуть безпосередньо спричиняти руйнування або пошкодження фізичних об'єктів і завдавати шкоди людям? Поясніть із точки зору міжнародних відносин.
17. Чи є підстави розглядати вплив кібер-засобами з точки зору міжнародного гуманітарного права?
18. Що таке "інформаційна війна"? А "кібервійна"?
19. У чому суть концепції інформаційного протиборства (Information Warfare)?
20. Які зміни відбуваються в західній концепції стртатегічних інформаційних упливів?
21. Якого підходу у військовій сфері інформаційної- та кібер-безпеки дотримується Україна?
22. Як взаємопов'язані військові й невійськові впливи в російській (східній) моделі інформаційної безпеки?
23. На чому базуються західний і східний підходи у сфері інформаційної безпеки?
24. Які історичні передумови сучасної концепції інформаційної безпеки в США?
25. На яких принципах ґрунтується політика Європейського Союзу у сфері інформаційної безпеки?
26. Яка концепція інформаційної безпеки реалізується в Японії?
27. У чому суть інформаційної безпеки з позицій Росії? Як це стосується свободи слова й інформації?
28. Що таке інформаційний- і кіберсуверенітет з точки зору Росії й Китаю?
29. Що таке "мережевий нейтралітет"? Яке ставлення до нього характерне для різних політичних систем?
30. У чому суть відмінностей у трактуванні поняття інформаційної безпеки?
31. У чому полягає проблемність застосування міжнародного права у сфері кібер-воєн?
32. Як співвідносяться поняття інформаційних- і кібер-воєн?
33. У чому полягає проблемність ідентифікації сторін конфлікту в умовах інформаційного протиборства з точки зору міжнародного права?
34. Яка роль Талліннського посібника у питанні застосування міжнародного права у сфері кібер-воєн?
35. Що таке "міжнародна інформаційна безпека"?
36. Що з позиції Росії розглядається в якості "загроз миру й безпеці в інформаційному просторі"?
37. У яких офіційних документах РФ відображено офіційні погляди на "міжнародну інформаційну безпеку"?
38. Що в Росії розглядають як "загрози міжнародній інформаційній безпеці"?
39. У чому суть зовнішньої політики Росії у сфері інформаційної безпеки?
40. У чому суть російського підходу до міжнародного співробітництва у сфері інформаційної безпеки?
41. У чому відмінність між поняттями "інформаційний простір" і "кіберпростір"?
42. Які головні напрями діяльності Росії на рівні ООН щодо просування своїх інтересів у сфері інформаційної (кібер) безпеки?
43. Як можна коротко окреслити сферу й обставини діяльності Групи урядових експертів у сфері інформатизації й телекомунікації в контексті міжнародної безпеки (UN GGE)?
44. У чому суть позиції Росії в сфері протидії інформаційній злочинності?

45. Яка причина особливої позиції РФ у сфері інформаційної (кібер) безпеки?

Китай

46. На яких засадах ґрунтується політика у сфері інформаційної (кібер) безпеки Китаю?
47. Яка інституційна основа політики інформаційної (кібер) безпеки КНР?
48. Як регулюється кіберпростір в КНР?
49. Як розвивалася нормативна основа кібербезпеки КНР?
50. У чому полягають головні виклики закону КНР про кібербезпеку з точки зору іноземних компаній?
51. У чому полягає системність підходу китайської влади до питання регулювання кіберпростору?
52. Які характерні риси були притаманні політиці кібербезпеки США у 2000-х рр.?
53. Які виклики визначали політику США у сфері кібербезпеки в період президентства Барака Обами?
54. Які цілі визначено у "Міжнародній стратегії для кіберпростору" США (2011 р.)?
55. Які характерні риси були притаманні політиці адміністрації Д. Трампа у сфері кібербезпеки?
56. Які позиції у сфері міжнародної політики характеризують кіберстратегію Д. Трампа?
57. Як змінилася політика США у сфері кібербезпеки з приходом адміністрації Джозефа Байдена?
58. Яка роль США в роботі Групи урядових експертів UN GGE?
59. Які наслідки діяльності Групи урядових експертів UN GGE та прийнятих нею рішень?
60. У чому суть ініційованої США Резолюції ГА ООН "Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки" (2018 р.)?
61. На яких засадах і з якою метою функціонує Робоча група відкритого складу, створена відповідно до Резолюції ГА ООН "Досягнення в сфері інформатизації й телекомунікацій у контексті міжнародної безпеки" (2018 р.)?
62. Які рішення прийнято UN GGE в період одночасної роботи з OEWG?
63. Які засади політики ЄС у сфері інформаційної (кібер) безпеки?
64. Яку роль відіграє політика кібербезпеки в Глобальній стратегії ЄС?
65. Як розвивається політика кібербезпеки ЄС?
66. Які головні положення Стратегії кібербезпеки ЄС для цифрового десятиліття (2020 р.)?
67. Які пріоритети в політиці кібербезпеки ЄС актуалізуються із прийняттям стратегії "Цифровий компас: європейський шлях до Цифрового десятиліття"?
68. На яких концептуальних підходах засновано сучасну стратегію ЄС у сфері кібербезпеки?
69. У чому суть пропозиції Програми дій для просування відповідальної поведінки держав у кіберпросторі і яка роль ЄС у її просуванні?
70. З якою метою проводиться Всесвітня інтернет-конференція і започатковано Уженьську ініціативу?
71. Які головні напрями міжнародної стратегії Китаю в кіберсфері?
72. Які головні напрями реалізації кіберстратегії Китаю в регіональних відносинах?
73. У чому полягають принципові відмінності між підходами до безпеки кіберпростору в Китаї та США?
74. У діяльності яких міжнародних організацій проявляється узгодження позицій Китаю та Росії в питаннях безпеки кіберпростору?
75. У чому суть протистояння між США й Китаєм у сфері кібербезпеки?
76. Який характер має конкуренція між США й Китаєм в аспекті кібер-можливостей?
77. Як формувалося розуміння Китаю як джерела кібер-загроз для США?
78. Як сьогодні розглядається Китай із точки зору кібер-безпеки США?
79. Із яких позицій влада Китаю розглядає США в аспекті кібер-безпеки?
80. Яка концептуальна позиція Європейського Союзу щодо політики у сфері безпеки кібер-простору?
81. Як узгоджуються зусилля ЄС і США у сфері міжнародної взаємодії щодо боротьби з кіберзлочинністю?
82. Які інституції функціонують у сфері співпраці ЄС і США щодо протидії кібер-загрозам?
83. Як здійснюється практична взаємодія ЄС і США і запозичення досвіду у сфері протидії кібер-загрозам?
84. Які розбіжності існують у підходах ЄС і США до політики безпеки кіберпростору?
85. Які проблеми безпеки кіберпростору покликана розв'язати кіберстратегія ЄС шляхом міжнародної взаємодії?
86. Які головні регіональні напрями міжнародної співпраці ЄС у сфері розвитку потенціалу протидії кібер-загрозам?
87. Які головні напрями співпраці держав ЄС у сфері кібербезпеки й оборони? 135
88. Як можна підсумувати головні проблеми міжнародного співробітництва у сфері інформаційної (кібер) безпеки?

IV. Політика оцінювання

Під час вивчення курсу використовується кіберсередовище Microsoft 365 (MS Teams та SharePoint). З цією метою заохочується використання мобільних пристроїв - застосовується підхід BYOD (Bring Your Own

Device). Під час проведення аудиторних занять здійснюється комунікація у віртуальному середовищі курсу в режимі реального часу. Фіксація часу роботи й активності здобувачів вищої освіти додатково фіксуються в автоматичному режимі. Завдання призначаються й оцінюються в середовищі команди курсу (MS Teams).

Відвідування та / або участь: відвідування та активна участь є класифікованою складовою курсу, що оцінюється, дистанційна он-лайн участь студента допускається за умови наявності у нього відповідних технічних засобів - у такому разі здійснюється онлайн-нарада в команді MSTeams.

Академічна доброчесність та співпраця: не допускається порушення норм авторського права, у разі виявлення плагіату письмова робота студента не оцінюється. Заохочується групова робота із презентацією її результатів у розділі "Простір для співпраці" персональних електронних блокнотів студентів.

Студенти з обмеженими можливостями: можуть брати дистанційну (онлайн) участь на підставі особистого звернення.

Заява про стан здоров'я студентів: у випадку погіршення стану здоров'я він, на підставі особистого письмового звернення (електронною поштою або в дописах команди MS Teams може брати дистанційну онлайн-участь у заняттях.

Затримки виконання: допускається за умови наявності непереборних обставин, що перешкоджали вчасному представленню, що підтверджується документально (наприклад, довідка лікаря).

Повторне оцінювання: допускається на підставі обґрунтованого письмового звернення студента (електронною поштою або в дописах команди MSTeams), але не пізніше як протягом одного тижня після основного оцінювання.

Політика відвідування та / або участі: відвідування та активна участь є оцінюваною складовою курсу

V. Підсумковий контроль

Підсумковий контроль у формі екзамену регулюється Положенням про організацію освітнього процесу на першому (бакалаврському) та другому (магістерському) рівнях у Волинському національному університеті імені Лесі Українки (https://ed.vnu.edu.ua/wp-content/uploads/2022/08/2022Polozhennya_pro_org_anizatsiyu_navch._pr_otsesu_u_VNU_%D1%80%D0%B5%D0%B4.pdf).

Максимальна кількість балів, яку може набрати здобувач освіти за поточну навчальну діяльність з освітнього компонента, становить 40 балів, підсумкова семестрова оцінка визначається як сума поточної семестрової та екзаменаційної оцінок у балах. Екзаменаційна оцінка визначається в балах за результатами виконання екзаменаційних завдань, за шкалою від 0 до 60.

Під час підсумкового контролю здобувач вищої освіти отримує:

– 50-60 балів, якщо він дає повну, вичерпну відповідь на поставлені запитання, вільно використовуючи поняття й терміни, що передбачені до вивчення, успішно вирішує ситуаційні завдання, наводить власні приклади, дає правильну відповідь на поставлені додаткові завдання, застосовуючи при цьому знання, здобуті при вивченні інших навчальних дисциплін, що передбачені програмою підготовки бакалавра за освітньо-професійною програмою «Міжнародна інформація та суспільні комунікації»;

– 38-49 бали, якщо відповідь студента на всі запитання є повною, але загалом має репродуктивний характер і містить незначну кількість несуттєвих недоліків;

– 26-37 балів, якщо відповідь загалом повна, але наявні значні недоліки з окремих питань;

– 14-25 балів, якщо відсутня відповідь на окремі запитання;

– 1-13 балів, якщо відповідь на окремі запитання фрагментарна, а на інші – відсутня;

– 0 балів, якщо відповідь відсутня.

Питання для підготовки до екзамену

1. Діяльність України на міжнародній арені у сфері інформаційної політики та безпеки
2. Інформаційна політика й безпека в стратегії національної безпеки України
3. Нормативно-правові акти в сфері інформаційної політики та безпеки України
4. Інституції у сфері інформаційної політики та безпеки України
5. Основні національні інтереси України в інформаційній сфері
6. Застосування загальних принципів міжнародного права до боротьби в інформаційній сфері
7. Міжнародне право збройних конфліктів і його придатність до дій в інформаційній сфері
8. Міжнародне гуманітарне право і його придатність до конфліктів із застосуванням інформаційних засобів
9. Національні підходи в питанні застосування права міжнародних конфліктів до інформаційної сфери
10. Переговорний процес і міжнародне співробітництво в галузі забезпечення інформаційної безпеки

11. Позиції й інтереси провідних акторів у сфері міжнародної інформаційної безпеки та управління інтернетом
12. Ініціативи в галузі інформаційної безпеки. Позиція США і країн Заходу
13. Ініціативи в галузі інформаційної безпеки. Позиція Росії
14. Розстановка сил на світовій арені у зв'язку з російськими та американськими ініціативами у сфері інформаційної/кібер-безпеки
15. Ініціативи в галузі інформаційної безпеки. Позиція Китаю
16. Ініціативи в галузі інформаційної безпеки. Позиція Європейського Союзу
17. Інформаційний тероризм і трансформація міжнародного тероризму
18. Міжнародне співробітництво щодо протидії кіберзлочинності
19. Інформаційна політика та безпека: підходи й концепції
20. Інформаційна політика держав. Координація міжнародної інформаційної політики
21. Виклики і загрози безпеки в інформаційну епоху
22. Інформаційно-технічні та соціо-гуманітарні аспекти інформаційної безпеки
23. Національні підходи до визначення інформаційної безпеки
24. Діяльність міжнародних організацій у сфері інформаційної політики
25. Офіційні документи міжнародних організацій у сфері інформаційної політики та безпеки
26. Суб'єкти інформаційного впливу - держави і недержавні гравці
27. Робота Комітетів ООН в галузі міжнародної інформаційної безпеки
28. Міжнародне співробітництво щодо забезпечення інформаційної безпеки: позиція України з питання інформаційної безпеки

.VI. Шкала оцінювання

Шкала оцінювання знань здобувачів освіти з освітніх компонентів, де формою контролю є іспит

Оцінка в балах	**Лінгвістична оцінка**	**Оцінка за шкалою ECTS**	
		оцінка	**пояснення**
90–100	Відмінно	A	відмінне виконання
82–89	Дуже добре	B	вище середнього рівня
75–81	Добре	C	загалом хороша робота
67–74	Задовільно	D	непогано
60–66	Достатньо	E	виконання відповідає мінімальним критеріям
1–59	Незадовільно	Fx	Необхідне перескладання

VII. Рекомендована література та інтернет-ресурси

Основна література

Копійка М.В. Модернізація політики міжнародних організацій у сфері інформаційної безпеки. Політичне життя. 2020. № 1. С. 102-109.

Федонюк Сергій. Міжнародні аспекти безпеки кіберпростору : монографія / С. В. Федонюк. – Луцьк : Вежа-Друк, 2022. – 1 електрон. опт. диск (CD-ROM). – Об’єм даних 4,72 Мб. ISBN 978-966-940-406-0

Федонюк Сергій, Карпук Ігор (2022). Концепції інформаційної безпеки в аспекті інтересів основних міжнародних акторів, Міжнародні відносини, суспільні комунікації та регіональні студії, № 2 (13).

Федонюк Сергій, Карпук Ігор (2022). Розвиток концепції стратегічних комунікацій ЄС, *Міжнародні відносини, суспільні комунікації та регіональні студії*, № 2 (13), с. 44-65.

Сергій Федонюк, Сергій Магдисюк. Протистояння між США й Китаєм у сфері кібербезпеки. Історико-політичні проблеми сучасного світу : Збірник наукових статей. – Чернівці: Чернівецький національний університет, 2022.–Т.45, с. 113–127.

Федонюк Сергій (2021). Політика ЄС в аспекті основних глобальних концепцій інформаційної (кібер) безпеки, *Міжнародні відносини, суспільні комунікації та регіональні студії*, № 3 (11)

Сергій Федонюк, Анна Ткачук. ФОНД “РУСКІЙ МІР” І ПРОСУВАННЯ ІДЕОЛОГІЇ КРЕМЛЯ // *Стратегічні комунікації в контексті безпекової політики: європейський і глобальний рівні:* матеріли Інтернет - конференції / за заг. ред. Н. Карпчук. – Луцьк: ВНУ імені Лесі Українки, 2022, с. 60-66.

https://stratcomeu.files.wordpress.com/2023/03/d09cd0b0d182d0b5d180-d0bad0bed0bdd184d0b5d180-19.05.22.pdf
Федонюк С.В., Оліферук В.В. Концепції інформаційної безпеки провідних міжнародних акторів. *Актуальні проблеми міжнародних відносин і регіональних досліджень* : матеріали Міжнародної науково-практичної інтернет-конференції (м. Луцьк, 6 грудня 2021 р.) / за ред. В. Й. Лажніка. – Луцьк : Вежа-Друк, 2021, с. 155-159. https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/39051/1/%D0%92%D0%98%D0%A8%D0%9D

Інтерактивний посібник
Федонюк Сергій. Міжнародна політика інформаційної (кібер) безпеки. 87 питань і відповідей : навч. посіб. / С. В. Федонюк. Рекомендовано рішенням вченої ради Волинського національного університету імені Лесі Українки від 23 лютого 2023 (протокол №1).
Веб-сайт посібника (https://internationalcybersecuritybook.wordpress.com/)

Додаткові джерела й документи
Книги, статті, документи (ресурси за покликанням доступні для всіх)
Політика безпеки кіберпростору (ресурси за покликанням доступні студентам ВНУ імені Лесі Українки)