

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

**СИЛАБУС**  
нормативної навчальної дисципліни  
**«МІЖНАРОДНА ІНФОРМАЦІЙНА БЕЗПЕКА»**

Підготовки бакалавра  
галузі знань 29 «Міжнародні відносини»  
Спеціальності 291 «Міжнародні відносини, суспільні комунікації  
та регіональні студії»  
Освітньо-професійна програма «Міжнародна інформація та суспільні  
комунікації»

Силабус розроблено на основі Програми нормативної навчальної дисципліни «Міжнародна інформація та суспільні комунікації», Стандарту вищої освіти України для бакалаврів спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії».

**Розробник:** к. географ. н., доц. Федонюк Сергій Валентинович

Силабус навчальної дисципліни затверджено на засіданні кафедри міжнародних комунікацій та політичного аналізу, протокол № 2 від 8 вересня 2020 р.

Завідувач кафедри:  (Карпчук Н.П.)

Волинський національний університет імені Лесі Українки  
Факультет міжнародних відносин  
Кафедра міжнародних комунікацій та політичного аналізу

СИЛАБУС

Міжнародна інформаційна безпека

Опис нормативної навчальної дисципліни



Найменування показників	Галузь знань, спеціальність, освітня програма, освітній рівень	Характеристика навчальної дисципліни
<b>Денна форма</b>	Галузь знань:	<b>Нормативна</b>
<b>180 год / 6 кредитів</b>	29 Міжнародні відносини	Рік навчання: 1
<b>ІНДЗ: €</b>	Спеціальність: 291 Міжнародні відносини, суспільні комунікації та регіональні студії <b>Освітньо-професійна програма:</b> Міжнародна інформація та суспільні комунікації <b>Освітній рівень:</b> Бакалавр	<b>Семестр: 1</b> <b>Лекції: 24</b> <b>Семінарські заняття: 30</b> <b>Самостійна робота: 114</b> <b>Консультації: 12</b> <b>Форма контролю:</b> екзамен
<b>Мова навчання: українська</b>		

2020-2021 н.р., I семестр

Група: МІ-12

Інформація про викладача

**Федонюк Сергій Валентинович**, кандидат географічних наук, доцент, доцент кафедри міжнародних комунікацій та політичного аналізу

**Контактна інформація** sergii.fedoniuk@vnu.edu.ua

**Локація** G-6

**Заняття:** Понеділок - 10.10 -11.30

**Години консультацій** Понеділок, вівторок - 15.00 -16.20

## **Анотація**

- Курс «Міжнародна інформаційна безпека» призначений для знайомства студентів з політологічними і нормативними підходами, сучасними тенденціями в оцінці значення проблеми інформаційної безпеки в міжнародному політичному процесі. Дає змогу визначити місце, особливості та основні тенденції трансформації глобальної безпеки в зв'язку з загальною інформатизацією, революцією у військовій справі і формуванням інформаційного суспільства, а також впливом цих тенденцій на зовнішню політику України та інших держав.
- Постреквізити. Цей курс є базовим для наступного формування компетенцій у сфері інформаційної безпеки.

## **Компетенції, що здобуваються**

### *Загальні компетенції:*

- володіння основними методами, способами і засобами отримання, зберігання, переробки інформації, навичками роботи з комп'ютером як засобом управління інформацією; здатністю працювати з інформацією в глобальних комп'ютерних мережах;
- уміння системно мислити, ставити цілі і вибирати шляхи їх досягнення, вміння знаходити міжнародно-політичні і дипломатичні смислові навантаження проблем і процесів;
- здатність ясно, логічно правильно і аргументовано будувати усну і письмову мову у відповідній професійній області;
- здатність розуміти суть і значення інформації в розвитку сучасного інформаційного суспільства, усвідомлювати небезпеку і загрози, що виникають в цьому процесі, дотримуватися основних вимог інформаційної безпеки, в тому числі захисту державної таємниці.

### *Професійні компетенції:*

- здатність розуміти логіку глобальних процесів і розвитку всесвітньої політичної системи міжнародних відносин в їх історичній, економічній та правовій обумовленості;
- здатність володіти базовими навичками прикладного аналізу міжнародних ситуацій;
- здатність розуміти зміст програмних документів з проблем зовнішньої політики України, уміння професійно грамотно аналізувати і пояснювати позиції України з основних міжнародних проблем.

## **Плановані результати навчання**

### *Знання:*

основні процеси, пов'язані з загальною інформатизацією; місце інформаційної безпеки в світових політичних процесах; логіку зміни і розвитку проблеми інформаційної безпеки;

### *Вміння:*

співвідносити глобалізаційні процеси і процеси інформатизації; визначати характер загроз, пов'язаних з процесом інформатизації;

### *Навички:*

- аналізу основних концептуальних підходів до проблеми забезпечення інформаційної безпеки, а також вміння аналізу конкретних подій у сфері безпеки в зв'язку зі зміною військових доктрин розвинених країн, революцією у військовій справі і загальною інформатизацією.

## **Навчальні ресурси**

- Для вивення курсу необхідне використання електронних освітніх ресурсів команди курсу на

платформі MS Teams за адресою:

<https://qr.go.page.link/Bekkp>



### Політика курсу

- **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 плагиату 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.
- **Мобільні пристрої:** заохочується використання мобільних пристроїв - застосовується підхід BYOD (Bring Your Own Device).

### Структура навчальної дисципліни

Тема	Предмет вивчення	Усього*	ЛК*	Семін*	Самост.*	Консуль*	Ф.К.**, бал
<b>Частина 1. Основи міжнародної інформаційної безпеки</b>							
1.1 Міжнародна інформаційна безпека: підходи до визначення поняття	Виклики і загрози безпеки в інформаційну епоху. Інформаційно-технічні та соціо-гуманітарні аспекти інформаційної безпеки. Міжнародна інформаційна безпека і кібер-безпека: порівняльний аналіз дослідницьких дискурсів та політичної практики. Національні підходи до	16	2	2	12		ДС

	визначення національної та міжнародної інформаційної безпеки. Підхід, зафіксований в офіційних документах ООН та інших міжнародних організацій. Принципи класифікації та джерела загроз МІБ. Тріада загроз міжнародній інформаційній безпеці: злочинна, терористична, військово-політична. Суб'єкти інформаційного впливу - держави і недержавні гравці.						
1.2 Інформаційне протиборство, інформаційні війни і конфлікти	Поняття «інформаційне протиборство», «інформаційна війна», «інформаційна зброя»: існуючі підходи до визначення. Інформаційні засоби впливу. Характеристика поняття «інформаційна зброя». Типізація інформаційної зброї. Технології впливу на критичні інформаційні інфраструктури держави. Технології кібершпіонажу. Потенціал впливу на громадську думку за допомогою соціальних мереж і Web 2.0 технологій.	15	1	2	12		ДС
1.3 Об'єкти інформаційної безпеки. Захист критичних інформаційних інфраструктур	Нові об'єкти безпеки в інформаційну епоху. Поняття «критична інформаційна інфраструктура». Визначення критичних інформаційних інфраструктур в різних країнах. 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.	15	1	2	12		ДС
1.4 Соціальні медіа, Web 2.0 технології та цифрова дипломатія в контексті інформаційної безпеки	Поняття і характеристики соціальних медіа та Web 2.0 технологій. Соціальні медіа та їх вплив на міжнародні та внутрішньодержавні конфлікти. Нові види загроз суспільній стабільності, пов'язані зшироким розповсюдженням соціальних мереж і Web 2.0 технологій. Цифрова дипломатія і використання соціальних медіа в дипломатичній практиці держав. Цифрова дипломатія в контексті міжнародної інформаційної безпеки.	15	1	2	12		ДС/ІН ДЗ
1.5 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.	19	1		18		ДС/ІР С
1.6 Міжнародне право в	Застосування загальних принципів міжнародного права до боротьби в інформаційній сфері. Міжнародне право збройних конфліктів і його	16	2	2	12		ДС/ Р/ІНД 3

аспекті інформаційної безпеки.	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 кібервоєн». 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 міжнародного права до інформаційної сфери.						
<b>Частина 2. Міжнародне співробітництво щодо забезпечення інформаційної безпеки</b>							
2.1 Ініціативи в галузі міжнародної інформаційної безпеки	Позиція США і країн Заходу. Позиція Росії. Російсько-американські відносини з питання міжнародної інформаційної безпеки. Позиція Китаю. Позиція України. Розстановка сил на світовій арені у зв'язку з російськими ініціативами по міжнародній інформаційній безпеці. Конференція в Дубаї 2012.	15	1	2	12		ДС/Р МГ
2.2 Переговорний процес і міжнародне співробітництво в галузі забезпечення інформаційної безпеки.	Робота Комітетів ООН з безпеки і роззброєння, по космосу, МСЄ, G7, Євросоюзу в галузі міжнародної інформаційної безпеки.	15	1	2	12		ДС
2.3 Перспективи формування глобального режиму міжнародної інформаційної безпеки	Позиції і інтереси провідних акторів у сфері міжнародної інформаційної безпеки та управління інтернетом. Співвідношення регіонального та глобального рівня міжнародної взаємодії щодо забезпечення інформаційної безпеки. Досвід міжнародного співробітництва в інших високотехнологічних областях світової політики (космос, контроль над ядерними озброєннями) і його придатність до інформаційної сфери. Перспективи формування глобального режиму міжнародної інформаційної безпеки та глобального управління інтернетом.	16	2	2	12		ДС/Р МГ
		142	12	16	114		

\* Кількість годин приведено у відповідність із наказом Східноєвропейського національного університету імені Лесі Українки від 28 травня 2020 р. № 142-з “Про затвердження норм часу для планування та обліку навчальної роботи та перелік основних видів методичної, наукової й організаційної роботи науково-педагогічних працівників на 2020/2021 н. р.”.

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

### Політика оцінювання

- **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.

### Оцінювання

Підсумкова оцінка складається з таких компонентів:

Види роботи	Частка у підсумковій оцінці, %
Присутність і робота на заняттях	20
Поточний контроль	20
Проміжний контроль	40
Підсумковий контроль	20

### Шкала оцінювання

Студентам будуть присвоєні такі підсумкові оцінки на основі загального підсумку набраних балів:

Оцінка	Відповідно до загальної кількості балів
Відмінно	90-100
Дуже добре	82-89
Добре	75-81
Задовільно	67-74
Достатньо	60-66
Незадовільно	0-59

## Рекомендована література та інтернет-ресурси

1. Макаренко ЄА., Рижков М.М., Ожеван М.А., Кучмій О.П., Фролова О.М. Міжнародна інформаційна безпека: теорія і практика. Підручник. – К. : Центр вільної преси, 2016. – 418 с.
2. Международная информационная безопасность: монография / Е.С.Зиновьева; Моск. гос. ин-т междунар. Отношений (ун-т) МИД России, каф. мировых политических процессов. — М.: МГИМО-Университет, 2013. — 194 с. — (Серия «Научная школа МГИМО»). ISBN 978-5-9228-1018-0.
3. Libicki M. Cyberdeterrence and cyberwar. Rand Corporation, 2009. URL: <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA508151>
4. The Tallinn Manual on the International Law Applicable to Cyber Warfare. / Ed. by Schmitt M. Cambridge University Press, 2013
5. Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace / K. Rausher, A. Korotkov. – 2011. – 75 p. – Mode of access : <http://www.ewi.info/working-towards-rules-governing-cyber-conflict>.
6. Mueller M. Are we in a digital cold war? / Internet Governance Project, 2013. – URL: <http://www.internetgovernance.org/wordpress/wp-content/uploads/DigitalColdWar31.pdf>