

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

**СИЛАБУС**  
вибіркової навчальної дисципліни  
**«ІНФОРМАЦІЙНА ТА КІБЕРБЕЗПЕКА»**

**Підготовки доктора філософії**  
**галузі знань 29 «Міжнародні відносини»**  
**Спеціальності 291 «Міжнародні відносини, суспільні комунікації**  
**та регіональні студії»**  
**освітньо-наукової програми «Міжнародна відносини та стратегічні комунікації**  
**України та ЄС»**

**Розробник:** к. політ. н., доц. Вознюк Євгенія Василівна

Силабус вибіркової навчальної дисципліни затверджено на засіданні кафедри міжнародних відносин і регіональних студій, протокол № 14 від 28.06.2022 р.  
Завідувач кафедри: Коцан Н. Н.

## СИЛАБУС

Найменування показників	Галузь знань, спеціальність, освітня програма, освітній ступінь	Характеристика навчальної дисципліни
форма навчання очна	галузь знань 29 Міжнародні відносини, спеціальність 291 "Міжнародні відносини, суспільні комунікації та регіональні студії", освітньо-професійна програма «Міжнародні відносини та стратегічні комунікації», доктор філософії	<b>Вибіркова</b>
Кількість годин/кредитів 120/4		<b>Рік навчання 1</b>
		<b>Семестр 2</b>
		<b>Лекції 10</b>
		<b>Практичні (семінарські) 14</b>
ІНДЗ: €		<b>Самостійна робота 88</b>
	<b>Консультації 8</b>	
		<b>Форма контролю: залік</b>
<b>Мова викладання</b>		<i>Українська</i>

### 1. ІНФОРМАЦІЯ ПРО ВИКЛАДАЧА

<b>ВИКЛАДАЧ</b>	Вознюк Є. В.
<b>КОНТАКТНІ ДАНІ</b>	Voznyuk.yevhenija@vnu.edu.ua
<b>КОМПЕТЕНЦІЇ ТА ДАНІ ПРО ВИКЛАДАЧА</b>	кандидат політичних наук, володіння українською, російською та англійською мовами (сертифікат B2). Наукові дослідження в сфері міжнародних відносин; місця та ролі України в сучасній системі міжнародних відносин, інформаційної та кібербезпеки.

### 2. ОПИС КУРСУ

<b>ПЕРІОД РЕАЛІЗАЦІЇ КУРСУ</b>	II семестр 2022 - 2023 навчального року
<b>ОРГАНІЗАЦІЙНА СТРУКТУРА</b>	Кафедра міжнародних комунікацій та політичного аналізу, факультет міжнародних відносин
<b>АНОТАЦІЯ КУРСУ</b>	Курс «Інформаційна та кібербезпека» призначений для знайомства аспірантів з трактування «інформаційної безпеки», «кібербезпеки», «інформаційного тероризму», «фейків», «дезінформації». Інформаційна та кібербезпека є надзвичайно гострим питанням розвитку та захисту громадян на сучасному етапі масового поширення гібридної війни, а особливо в процесі війни, розв'язаної росією на території України.
<b>ФОРМА РЕАЛІЗАЦІЇ</b>	<i>Лекцій-10 год., сем.-14 год.</i>
<b>МЕТОДИ ТА ФОРМИ ОЦІНКИ РОБОТИ СТУДЕНТІВ</b>	Формою підсумкового семестрового контролю з даної дисципліни є залік, що складається в усній формі. Залік виставляється за умови, якщо аспірант виконав усі види навчальної роботи, які визначені програмою навчальної дисципліни та отримав не менше 60 балів. У випадку незадовільної підсумкової оцінки, або за бажанням підвищити

	рейтинг, аспірант може добрати бали на заліку, виконавши певний вид робіт. Оцінка та засвоєння курсу виставляються згідно шкали оцінювання
<b>ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦІПЛІНИ</b>	Оцінювання під час семінарських занять здійснюється на основі того наскільки аспірант вміє самостійно проаналізувати і передати здобуті знання, перечитування інформації з листка забороняється. Посилання на використані матеріали та ресурси є обов'язковими, кожен аспірант несе особисту відповідальність за академічну доброчесність. Пропущені лекційні заняття не відпрацьовуються, семінарські заняття можуть бути відпрацьованими лише за умови наявності вагомих доказових причин відсутності аспіранта. Дедлайн здачі пропущених семінарських занять (за умови вагомих доказових причин) до дня здачі заліку. Максимальна кількість пропусків без вагомих доказових причин – 2.
<b>МЕТА І ЗАВДАННЯ І КУРСУ</b>	<b>Метою курсу</b> є формування знань про загальні закономірності, тенденції, специфічні риси і особливості історичного формування, функціонування та розвитку інформаційної та кібербезпеки світу; основи інформаційної та кібербезпеки країн Європи, Азії, Африки, Америки: нормативно-правова база, державно-організаційний апарат, сучасні проблеми, загрози, шляхи вирішення та перспективні засоби забезпечення; особливості інформаційних війн у сучасному світі; загрози інформаційній безпеці в мережі Інтернет; дезінформація та інформаційний тероризм; тенденції й проблеми розповсюдження інформаційного (кібер-) тероризму та інформаційна безпека світу; кібер- та інформаційна безпека України в умовах російської агресії. <b>Основними завданнями курсу</b> є підготовка фахівців, здатних розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної та/або кібербезпеки.
<b>ПРЕРЕКВІЗИТИ</b>	базові знання основних норм та правил інформаційної, кібербезпеки, інформаційної гігієни.
<b>ПОСТРЕКВІЗИТИ</b>	Цей курс є базовим для наступного формування компетентностей у сфері інформаційної безпеки, вивчення сучасних проблем міжнародних відносин та глобального розвитку.

### 3. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦІПЛІНИ

Назви змістових модулів і тем	Кількість годин				
	Усього	у тому числі			Консул.
		Лек.	Сем, практ.	Сам. роб	
1	2	3	4	5	6
<b>Змістовий модуль 1. Інформаційна безпека як важлива складова реалізації державної політики</b>					
Тема 1. Теоретичні та методологічні основи захисту інформації	18	1	2	14	1
Тема 2. Структура законодавства в сфері захисту інформації	19	2	2	14	1
Тема 3. Порядок і правила захисту інформації	18	1	2	14	1
Разом за змістовим модулем 1	55	4	6	42	3

<b>Змістовий модуль 2. Кібербезпека та собливості її реалізації</b>					
Тема 4. Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку	19	2	2	14	1
Тема 5. Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки	19	2	2	14	1
Тема 6. Стандарти інформаційної та кібернетичної безпеки	27	2	4	18	3
Разом за змістовим модулем 2	65	6	8	46	5
<b>Усього години</b>	<b>120</b>	<b>10</b>	<b>14</b>	<b>88</b>	<b>8</b>

#### **4. ТЕМАТИКА СЕМІНАРІВ / ПРАКТИЧНИХ / ЛАБОРАТОРНИХ РОБІТ**

<b>Назви змістових модулів і тем</b>	<b>год.</b>
<b>Змістовий модуль 1. Інформаційна безпека як важлива складова сучасного життя суспільства</b>	
Тема 1. Теоретичні та методологічні основи захисту інформації 1 Базові поняття у галузі інформаційної безпеки. 2 Складові інформаційної безпеки. 3 Характеристика інформації як предмета захисту. 4 Інформація як об'єкт права власності. 5 Сутність та цілі захисту інформації. 6 Циклічна модель інформаційної безпеки. 7 Потенційні загрози безпеки інформації та їх класифікація.	2
Тема 2. Структура законодавства в сфері захисту інформації 1 Загальна характеристика законодавчих актів в сфері захисту інформації. 2 Захист інформації як об'єкт адміністративно-правового регулювання. 3 Система органів регулювання технічного захисту інформації України. 4 Взаємодія суб'єктів системи технічного захисту інформації. 5. Напрями реалізації державної політики у сфері захисту інформації. 6. Ліцензування господарської діяльності у галузі захисту інформації. 7. Дозвільна система проведення робіт у галузі технічного захисту інформації	2
Тема 3. Порядок і правила захисту інформації 1 Етапи життєвого циклу засобів захисту інформації та їх характеристика. 2 Питання сертифікації продукції в сфері захисту інформації. 3 Державна експертиза у сфері захисту інформації. 4. Класифікація автоматизованих систем в НД ТЗІ. 5. Моделі захисту інформації в автоматизованій системі. 6. Модель порушника інформаційної безпеки. 7. Порядок і правила захисту інформації в КС/АС. 8. Забезпечення доступності й цілісності інформації в АС.	2
<b>Змістовий модуль 2. Кібербезпека та собливості її реалізації</b>	
Тема 4. Законодавство про шифрування, цифровий підпис та органи спеціального зв'язку 1 Предмет криптографії. 2 Криптосистеми та загрози їх безпеки. 3 Симетричні та асиметричні криптосистеми. 4 Формування та перевіряння електронного цифрового підпису. 5 Порядок забезпечення криптографічного захисту інформації.	2

<p>Тема 5. Світовий досвід нормативного регулювання у сфері інформаційної та кібернетичної безпеки</p> <p>1 Провідні світові та національні органи зі стандартизації.</p> <p>2 Нормативне регулювання у сфері інформаційної безпеки в ЄС.</p> <p>3 Підходи країн ЄС та НАТО щодо регулювання питань кібернетичної безпеки</p>	2
<p>Тема 6. Стандарти інформаційної та кібернетичної безпеки</p> <p>1. Сімейство стандартів інформаційної та кібернетичної безпеки.</p> <p>2 Структура стандарту по кібербезпеці.</p> <p>3 Базові блоки стандарту ISO 27032.</p> <p>4 Заходи забезпечення кібербезпеки.</p> <p>5 Основи обміну інформацією та координації.</p> <p>Представити перед аудиторією виконане ІНДЗ та обґрунтувати його результати та доцільність</p>	4
<b>Усього годин</b>	<b>14</b>

### 5. ІНДИВІДУАЛЬНЕ НАУКОВО-ДОСЛІДНЕ ЗАВДАННЯ

Провести аналітичне дослідження і написати реферативний огляд на тему «Проблеми та перспективи реалізації сучасної інформаційної та кібербезпеки в державих світу» (держава виноситься на вибір аспіранта і не повинна повторюватися в групі).

### 6. РЕЗУЛЬТАТИ НАВЧАННЯ

	Інтегральна	Загальні	Фахові	
		ЗК12	СК2	СК9
<b>Компетентності</b>	Здатність розв'язувати складні спеціалізовані завдання та практичні проблеми в сфері міжнародних відносин, суспільних комунікації та регіональних студій, зовнішньополітичної діяльності держав, міжнародних взаємодій між державами, міжнародними організаціями та недержавними акторами, що характеризуються комплексністю та невизначеністю умов та передбачає застосування теорій суспільних наук та спеціальних	Здатність до пошуку, оброблення та аналізу інформації з різних джерел	Здатність аналізувати міжнародні процеси у різних контекстах, зокрема політичному, безпековому, правовому, економічному, суспільному, культурному та інформаційному.	Здатність застосовувати знання та характеристик розвитку країн та регіонів, особливостей та закономірностей глобальних процесів та місця в них окремих держав для розв'язання складних спеціалізованих задач і проблем

	наукових методів дослідження проблем міжнародних відносин.			
--	--	--	--	--

<b>Програмні результати</b>	<b>РН04</b>	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.
	<b>РН17</b>	Мати навички самостійного визначення освітніх цілей та навчання, пошуку необхідних для їх досягнення освітніх ресурсів.

## 7. РОЗПОДІЛ БАЛІВ

Модуль 1							Модуль 2	Сума балів
Змістовий модуль 1			Змістовий модуль 2					
1	2	3	4	5	6	7	ІНДЗ	
10	10	10	10	10	10	10		
30			40					
<b>70 балів</b>							<b>30</b>	<b>100</b>

## 8. ШКАЛА ОЦІНЮВАННЯ

Оцінка в балах за всі види навчальної діяльності	Оцінка для заліку
90 – 100	Зараховано
82 – 89	
75 - 81	
67 -74	
60 - 66	
1 – 59	Незараховано (з можливістю повторного складання)

## 9. РЕКОМЕНДОВАНА ЛІТЕРАТУРА

<b>Методичне забезпечення</b>	<ol style="list-style-type: none"> <li>1. Вознюк Є. В. Інформаційний тероризм VS міжнародна безпека. Монографія. Луцьк: Вежа-друк, 2021. 223 с.</li> <li>2. Vozniuk E. Information Terrorism as a Modern Dynamic Part of International Terrorism. <i>International and National Security: Politics, Information, Ecology, Economy: collective monograph</i> / ed. by A. Mytko. Kyiv : MPBP «Hordon», 2018. 320 p. (P. 165-174).</li> </ol>
<b>Основна</b>	<ol style="list-style-type: none"> <li>1. Вознюк Є. Секрет успіху США у сфері інформаційної безпеки. Міжнародні відносини, суспільні комунікації та регіональні студії, 2018. №1(3). С. 66–71.</li> <li>2. Vozniuk E. Information Security of India. Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія : Міжнародні відносини. 2018.</li> <li>3. Вознюк Є. Кібербезпека в умовах російської агресії Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія : Міжнародні відносини. 2020. №2 (406).</li> <li>4. Vozniuk E. Principles and features of Japan's information security system. Журнал «Політичне життя», Донецького національного університету імені Василя Стуса, №4, 2017 р.</li> <li>5. Vozniuk E. The Problems of Informational Terrorism in African Countries. «Studia Humanitatis». 2019 [Електронне видання]. – Режим доступу: <a href="http://st-hum.ru/content/vozniuk-ev-problems-informational-terrorism-african-countries">http://st-hum.ru/content/vozniuk-ev-problems-informational-terrorism-african-countries</a>.</li> <li>6. Вознюк Є. Розвиток кібербезпеки Бразилії на сучасному етапі Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія : Міжнародні відносини. 2020. №2 (406).</li> <li>7. Вознюк Є. Поширення впливу мексиканських картелів засобами інформаційних технологій і пропаганди. Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Серія : Міжнародні відносини. 2019. №8 (392). С.35–41.</li> <li>8. Вознюк Є. The Influence of the Information Society Development on Political Ideologies <i>Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate</i>. 11(1) (2021). DOI 10.24917/26578549.11.1.2.</li> <li>9. International information security AD ALTA: Journal of Interdisciplinary Research. volume 11, issue 01. 429 pages. DOI 10.33543/1101.</li> <li>10. Вознюк Є. Особливості поширення російських фейків в Україні. Історико-політичні проблеми сучасного світу: Збірник наукових статей. Чернівці: Чернівецький національний університет, 2021. Т. 44. С. 52-64. DOI: 10.31861/mhpi2021.44.52-63</li> <li>11. Вознюк Є. Фейк російської пропаганди: Олена Підгрушна – снайпер АТО. Міжнародні відносини, суспільні комунікації та регіональні студії. 2021. № 1 (9). С.83-101</li> <li>12. Вознюк Є. Громадські об'єднання на захисті інформаційного простору України Міжнародні відносини, суспільні комунікації та регіональні студії. № 3 (11).2021. с.48-61.</li> <li>13. Вознюк Є. SWOT-аналіз стану інформаційної безпеки України Науковий часопис НПУ імені М.П. Драгоманова. Серія 22. Політичні</li> </ol>

	<p>науки та методика викладання соціально-політичних дисциплін, 22(30), 2021. <a href="https://doi.org/10.31392/pnspd.v22i30.1147">https://doi.org/10.31392/pnspd.v22i30.1147</a>.</p> <p>14. Вознюк Є. Нормативно-правове регулювання інформаційної безпеки США. Проблеми та перспективи наукових досліджень / Матеріали LX Міжнародної науково-практичної конференції, Чернівці, 15-16 червня 2018 р. – Київ: Науково-видавничий центр «Лабораторія думки», 2018. – 31 с.</p>
<p><b>Додаткова</b></p>	<ol style="list-style-type: none"> <li>1. Даценко А. Ю. Європейський досвід протидії російській дезінформації періоду другої «холодної війни». Міжнародні відносини. Серія «Політичні науки». No 18–19 (2018). URL: <a href="http://journals.iir.kiev.ua/index.php/pol_n/article/view/3381">http://journals.iir.kiev.ua/index.php/pol_n/article/view/3381</a></li> <li>2. Фролова О. Міжнародне співробітництво в галузі забезпечення інформаційної безпеки. Вісник Львівського університету. Серія: Міжнародні відносини. Вип. 46. 2019. С. 123–136. URL: <a href="http://nbuv.gov.ua/UJRN/VLNU_Mv_2019_46_13">http://nbuv.gov.ua/UJRN/VLNU_Mv_2019_46_13</a></li> <li>3. Kushnir, V. Proposals for improving the legal mechanism on strategic communications in the armed forces of Ukraine, Derzhavne upravlinnya: udoskonalennya ta rozvytok. Vol. 10, 2020. URL: <a href="http://www.dy.nayka.com.ua/?op=1&amp;z=1796">http://www.dy.nayka.com.ua/?op=1&amp;z=1796</a></li> <li>4. Géry Aude A New UN Path to Cyber Stability. Directions. Cyber Digital Europe, 6 October 2020. URL: <a href="https://directionsblog.eu/a-new-un-path-to-cyber-stability/">https://directionsblog.eu/a-new-un-path-to-cyber-stability/</a></li> <li>5. Taylor Emily, Hoffmann Stacie EU–US Relations on Internet Governance. Chatham House. 2019. URL: <a href="https://www.chathamhouse.org/publication/eu-us-relations-internet-governance">https://www.chathamhouse.org/publication/eu-us-relations-internet-governance</a>.</li> </ol>