

Код та назва дисципліни українською мовою / Назва дисципліни англійською мовою	2-СЗ-291-3 Кібербезпековий ландшафт в транснаціональному вимірі / Cybersecurity landscape in a transnational dimension
Рекомендується для галузі знань (<i>спеціальності, освітньої програми</i>)	
Кафедра (<i>зазначити повну назву кафедри</i>)	кафедра міжнародних відносин
П.І.П. НПП (<i>за можливості</i>)	доц. Головка І.К.
Рівень ВО	другий (магістерський)
КУРС, семестр (<i>в якому буде викладатись</i>)	
Мова викладання	українська
Пререквізити (<i>передумови вивчення дисципліни</i>)	
Чому це цікаво/треба вивчати	У цифрову епоху кібербезпека стала ключовим елементом міжнародної безпеки. Кібератаки та інформаційні загрози мають транснаціональний характер і потребують глобального реагування. Вивчення дисципліни дозволяє зрозуміти сучасні кіберзагрози, роль держав і міжнародних організацій у сфері кібербезпеки та формує важливі навички для роботи у сфері міжнародних відносин і безпеки.
Перелік тем з дисципліни	1.Цифрова трансформація та нові виклики для міжнародної безпеки 2.Кіберпростір як новий вимір глобальної політики 3.Основні типи кіберзагроз: хакерство, кібершпигунство, кібератаки 4.Державна кіберстратегія: політики США, Китаю, ЄС. 5.Міжнародне право і кібербезпека: нормативні прогалини та ініціативи 6.Роль ООН, НАТО, ЄС та інших міжнародних акторів у кібербезпеці 7.Кібердипломатія: новий інструмент зовнішньої політики 8.Кібертероризм і гібридні загрози: транснаціональні ризики 9.Захист критичної інфраструктури в міжнародному контексті 10. Транснаціональне співробітництво та виклики цифрового суверенітету
Як можна користуватися набутими знаннями і уміннями (<i>компетентність</i>)	Набуті знання та вміння дозволяють аналізувати глобальні кіберзагрози, орієнтуватися в нормативно-правовому полі кібербезпеки, брати участь у розробці політик

	цифрової безпеки та міжнародного співробітництва. Студент здобуває компетентності, необхідні для роботи у сферах міжнародних відносин, безпеки, кібердипломатії, а також в аналітичних центрах і міжнародних організаціях, що займаються цифровим врядуванням і захистом інформаційного простору.
Очікувані результати навчання	Після завершення курсу студент розумітиме структуру сучасних кіберзагроз і роль міжнародних акторів у забезпеченні кібербезпеки. Умітиме аналізувати політики та стратегії держав у цифровій сфері, орієнтуватися в міжнародному праві кіберпростору та застосовувати знання у сфері кібердипломатії. Студент також здобуде навички аналітичної роботи, стратегічного мислення та міжкультурної взаємодії в умовах цифрових загроз.
Інформаційне забезпечення	Курс базується на звітах міжнародних організацій (ООН, НАТО, ЄС, ITU), наукових публікаціях з кібербезпеки, документах з національних кіберстратегій, матеріалах з кіберправа та цифрової дипломатії. Додатково використовуються аналітичні ресурси (CSIS, CyberPeace Institute), електронні бази (Scopus, JSTOR), а також онлайн-курси з платформ Coursera, edX та матеріали профільних конференцій. Навчальні матеріали доступні через освітню платформу університету.
Види навчальних занять (<i>лекції, практичні, семінарські, лабораторні заняття тощо</i>)	Лекції, семінарські заняття
Вид семестрового контролю	Диференційований залік
Максимальна кількість здобувачів на семестр / Мінімальна кількість здобувачів (тільки для мовних, творчих дисциплін, за необхідності)	Без обмежень

Декан факультету _____

Віталій КРИВОШЕЇН