СИЛАБУС
«Міжнародне інформаційна безпека»

Викладач
Доценко Олена Михайлівна
кандидат юридичних наук
е-пошта: olena.dotsenko@karazin.ua
телефон: 0662847282
часи роботи: _____

Академічний період
1 семестр 2020/2021 н.р.
Академічні години
Вівторок 18.40
Місце проведення
Дистанційно
Навчальне навантаження
3 кредити ЄКТС, 90 годин

Пререквізити: здобувачі повинні мати знання з дисциплін «Актуальні проблеми міжнародних відносин та глобального розвитку», «Міжнародні організації в сфері безпеки», орієнтуватись у загальних тенденціях розвитку міжнародних відносин, вільно володіти державною мовою.

Постреквізити: вивчення дисципліни сприяє формуванню у здобувачів базових знань щодо основних понять, методів, підходів та тенденцій міжнародної інформаційної безпеки, а також практичних умінь та навичок визначення місця, особливостей і основних тенденцій трансформації безпеки в сучасній світовій політиці у зв'язку із загальною інформатизацією і формуванням інформаційного суспільства, правильного тлумачення та застосування міжнародних нормативно-правових актів, необхідних для їх майбутньої трудової діяльності як фахівців у сфері міжнародної інформаційної безпеки.

Призначення навчальної дисципліни: навчальна дисципліна призначена для підготовки магістрів за спеціальністю 291 «Міжнародні відносини, суспільні комунікації та регіональні студії» «освітньо-професійної програми «Міжнародна інформаційна безпека». Вивчення дисципліни передбачає формування наступних фахових компетентностей:

ФК 1. Поглиблені знання про природу, динаміку, принципи організації міжнародних відносин, типи та види міжнародних акторів, сучасні тенденції розвитку світової політики.

ФК 3. Здатність аналізувати та прогнозувати міжнародні відносини у різних контекстах, зокрема політичному, безпековому, правовому, суспільному, культурному та інформаційному.

ФК 4. Поглиблені знання про теоретичні та прикладні дослідження міжнародних відносин і світової політики у політичній, економічній, юридичній науках, у міждисциплінарних дослідженнях.

ФК 7. Здатність провадити прикладні аналітичні розробки проблем міжнародних відносин та світової політики, фахово готувати аналітичні матеріали та довідки.

ФК 11. Здатність виробляти підходи до розв'язання проблем і завдань у сфері міжнародних відносин, міжнародної та національної безпеки, зовнішньої політики (зокрема, міжнародних та внутрішньодержавних конфліктів).

Цілі курсу:
ПРН 35 – знання сучасних концепцій та стратегій міжнародної інформаційної безпеки.
ПРН 42 – володіти сучасними концепціями та стратегіями міжнародної інформаційної безпеки.
ПРН 49 – використовувати сучасні концепції та стратегії міжнародної інформаційної безпеки.

Інформаційні ресурси:

Необхідні

1) Грицун О. О. Поняття міжнародної інформаційної безпеки: порівняльно-правовий аспект. *Науковий вісник Ужгородського національного університету.* Серія ПРАВО. 2015. Випуск 31. Том 3. С. 123–127. URL: http://www.visnyk-juris.uzhnu.uz.ua/file/No.31/part_3/33.pdf (дата звернення: 20.08.2020).
2) Інформаційна безпека (соціально-правові аспекти) / В. Остроухов, В. Петрик, М. Присяжнюк та ін. ; за ред. Є.Д. Скулиша. К. : КНТ, 2010. 776 с.
3) Лапінська Є. І. Інформаційна безпека: поняття, види та ознаки. *Порівняльно-аналітичне право.* 2018. № 6. С. 262–266.
4) Макаренко Є. А. Міжнародне співробітництво у сфері інформаційної безпеки: регіональний контекст. *Актуальні проблеми міжнародних відносин.* 2011. Випуск 102 (Частина І). С. 160–164.
5) Міжнародна та національна безпека: теоретичні і прикладні аспекти : матер. III Міжнар. наук.-практ. конф. (м. Дніпро, 15 бер. 2019 р.). Дніпро : Дніпроп. держ. ун-т внутр. справ, 2019. 365 с. URL: https://dduvs.in.ua/wp-content/uploads/files/Structure/science/publish/np2d5.pdf (дата звернення: 20.08.2020).
6) Терещук В. І. Міжнародні комунікації у безпековому дискурсі ООН: наявні і потенційні виклики. *Міжнародні відносини. Серія «Політичні науки».* 2019. № 21. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3874/3534 (дата звернення: 10.05.2020).
7) Ткачук Т. Ю. Правове забезпечення інформаційної безпеки в умовах Євроінтеграції України: дис. … докт. юрид. наук: 12.00.07 / ДВНЗ «Ужгородський національний університет. Ужгород, 2019. 487 с.
8) Толубко В. Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти) : монографія. Київ : НАОУ, 2003. 320 с.
9) Andress J. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. 2nd ed. Syngress, 2014. 240 p.
10) Giacomello G. Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. 1st ed. Bloomsbury Academic, 2014. 256 p.

Додаткові

1) Близнюк А. Гібридна війна XXI століття. Пропаганда як основна складова у політичних, соціальних та етнічних протистояннях. *Інтермарум: історія, політика, культура.* 2015. Вип. 2. С. 390–399.
2) Бойко С. Проблематика международной информационной безопасности на площадках ШОС и БРИКС. *Международная жизнь* : веб-сайт. 23.01.2019. URL: https://interaffairs.ru/news/show/21480 (дата звернення: 20.08.2020).
3) Валюшко І. О. Інформаційна безпека України в контексті російсько-українського конфлікту: дис. … канд. політ. наук: 23.00.04 / Дипломатична академія України при МЗС України; Чорноморський національний університет імені Петра Могили. Київ, 2018. 210 с.
4) Любохинець Л. С., Поплавська О. В. Світова практика забезпечення інформаційної безпеки в сучасному глобалізованому середовищі. *Науково-виробничий журнал «Бізнес-навігатор».* 2017. Випуск 4-1 (43). С. 93–97.
5) Почепцов Г. Г. Сучасні інформаційні війни. Київ: Києво-Могилянська академія, 2015. 498 с.
6) Сербіна К. Ю. Необхідність реформування безпекового простору у контексті протидії новим викликам безпеці (на прикладі діяльності організації американських держав). *Актуальні проблеми міжнародних відносин.* 2012. Випуск 107 (Частина ІІ). С. 151–161.

7) Яцишин М. Ю. Роль міжнародних організацій у протидії кіберзлочинності. Українське право. 15.12.2019. URL: https://ukrainepravo.com/international_law/public_international_law/rolmizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/ (дата звернення: 20.08.2020).
8) About CSIRTs Network. *CIRTsNEtwork* : web-site. URL: https://csirtsnetwork.eu/ (Last Accessed: 20.08.2020).
9) About ENISA. *ENISA* : web-site. URL: https://www.enisa.europa.eu/about-enisa (Last Accessed: 20.08.2020).
10) About Us. *CERT-EU*. URL: https://cert.europa.eu/cert/plainedition/en/cert_about.html (Last Accessed: 20.08.2020).

Політика курсу:

- відвідування занять є обов'язковим елементом вивчення курсу, проте бали за відвідування без виконання завдань та роботи на практичному занятті не ставляться;
- розподіл навчального навантаження: курс передбачає 10 годин лекцій, 10 годин практичних занять та 70 годин самостійної роботи;
- виконання завдань, процедури подання завдань на перевірку, кінцевих термінів здачі завдань, запізнення здачі контрольних робіт, повторної здачі завдань: здобувачі виконують та здають на перевірку завдання, передбачені робочою програмою та комплексом навчально-методичного забезпечення дисципліни протягом семестру підчас практичних занять або консультацій, граничний строк подачі завдань на перевірку – останнє заняття. У разі повторної здачі завдання після зауважень, кількість балів, які може отримати здобувач, знижується на 20% від максимальної кількості балів за конкретне завдання.
- пропуски занять: для відпрацювання пропущеного практичного заняття здобувач має відповісти на теоретичні питання за темою, що відпрацьовує, а також здати письмові завдання за темою на оцінювання в день відпрацювання. Граничний строк відпрацювання пропущених занять – остання консультація перед екзаменом;
- академічна мобільність: відпрацювання пропущених занять або перезарахування результатів навчання в іншому закладі з причини академічної мобільності здійснюється відповідно до чинного законодавства України та внутрішніх нормативних документів ХНУ імені В. Н. Каразіна;
- перезарахування результатів навчання в іншому закладі: здійснюється відповідно до чинного законодавства України та внутрішніх нормативних документів ХНУ імені В. Н. Каразіна, а також за умови усної відповіді здобувачем на 3 питання за будь-якими темами курсу;
- дотримання академічної доброчесності, плагіату, наслідків порушення академічної доброчесності: дотримання академічної доброчесності є однією з основних вимог при виконанні завдань, підготовці до занять, роботи на практичних заняттях та написання екзаменаційної роботи. У разі недотримання академічної доброчесності вживаються заходи відповідальності, передбачені чинним законодавством України;
- вивчення дисципліни особами з особливими вимогами: здійснюється в звичайному форматі з індивідуальним підходом до здобувача та врахуванням особливих вимог;
- поведінка в аудиторії (запізнення, їжа, напої): здобувачі мають дотримуватися етичних норм у навчанні, поважати своїх колег. У разі запізнення до 15 хвилин, здобувач може зайти до аудиторії, не відволікаючи інших від роботи. Запізнення понад 15 хвилин вважається пропуском та має бути відпрацьоване. Під час навчання мають бути дотримані етичні норми, протягом заняття можна вживати воду, проте не вживати їжу;

- використання електронних пристроїв: під час проведення лекцій та практичних занять здобувачам дозволяється використання електронних пристроїв, але виключно в якості допоміжного інструменту для навчання.

Протоколи комунікації

Здобувачі можуть обмінюватися інформацією з викладачам під час лекцій, практичних занять та консультацій, а також за допомогою сайту дистанційного навчання https://dist.karazin.ua/moodle, електронної пошти викладача olena.dotsenko@karazin.ua, месенджера Telegram 0939026266. Електронні засоби комунікації слід застосовувати у робочі дні та робочий час викладача.

Форми контролю та критерії оцінювання

Поточний контроль знань здобувачів проводиться на *практичному занятті у формі усного опитування та навчальної дискусії, виконання тестових завдань, захисту презентацій доповідей, навчальних дискусій за науковою статею та нормативними актами, захисту есе, колоквіуму* тощо.

Сума балів за виконання завдань на практичному занятті складає:

Тема 1 – 3,5 бали: (захист презентацій доповідей – 1 бал; навчальна дискусія за науковою статею – 1,5 бали; захист есе – 1 бал).

Тема 2 – 3 бали: (захист презентацій доповідей – 1 бал; виконання тестових завдань – 1 бал; захист есе – 1 бал).

Тема 3 – 3 бали: (захист презентацій доповідей – 1 бал; виконання тестових завдань – 1 бал; захист есе – 1 бал).

Тема 4 – 12 балів: (захист презентацій доповідей – 2 бали; виконання тестових завдань – 1 бал; навчальні дискусії за нормативними актами – 3 бали; захист есе – 1 бал; колоквіум – 5).

Поточний контроль *самостійної роботи здобувачів проводиться у формі підготовки відповідей за навчальними питаннями теми, підготовки презентацій доповідей, підготовки тематичних схем, підготовки есе, аналізу статей, аналізу нормативних актів, групової роботи з підготовки питань для колоквіуму.*

Сума балів за виконання завдань для самостійної роботи здобувачів складає:

Тема 1 – 8,5 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; підготовка презентацій доповідей – 2 бали; підготовка тематичної схеми – 1 бал; аналіз статті – 1,5 бали; підготовка есе – 2 бали.

Тема 2 – 7 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; підготовка презентацій доповідей – 2 бали; підготовка тематичної схеми – 1 бал; підготовка есе – 2 бали.

Тема 3 – 7 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; підготовка презентацій доповідей – 2 бали; підготовка тематичної схеми – 1 бал; підготовка есе – 2 бали.

Тема 4 – 16 балів: підготовка відповідей за навчальними питаннями теми – 2 бали; підготовка презентацій доповідей – 4 бали; підготовка тематичної схеми – 1 бал; аналіз нормативних актів – 3 бали; підготовка есе – 2 бали; групова робота з підготовки питань до колоквіуму – 4.

Загальна сума балів за виконання завдань для самостійної роботи та роботу на практичних заняттях може сягати 60 балів.

Підсумковий семестровий контроль проводиться у формі заліку. Вміст залікового білета й оцінювання відповідей на залiку: 40 тестових завдань. Максимальна кількість балів – 40 (правильна відповідь на 1 тестове завдання = 1 бал).

У разі використання заборонених джерел на заліку здобувач на вимогу викладача залишає аудиторію та одержує загальну нульову оцінку (0 балів).

У разі настання / подовження дії **обставин непоборної сили** (в тому числі запровадження жорстких карантинних обмежень в умовах пандемії з забороною відвідування ЗВО) здобувачам вищої освіти денної та заочної форм навчання надається можливість скласти залік **у такій самій формі дистанційно на платформі Moodle** в дистанційному курсі «Міжнародна інформаційна безпека».

Критерії оцінки успішності та результатів навчання

Критеріями оцінювання знань за поточний контроль є рівень засвоєння знань та набуття навичок на лекціях та практичних заняттях, що включає систематичність їх відвідування, здатність здобувача засвоювати категорійний апарат, вміння орієнтуватися у сучасних подіях в світі і державі, навички узагальненого мислення, логічність та повноту засвоєння навчального матеріалу, навички творчого підходу до вирішення поставлених завдань, активність роботи на практичних заняттях, рівень знань за результатами опитування на практичних заняттях, самостійне опрацювання тем в цілому чи окремих питань.

Розрахункова шкала для оцінювання роботи здобувачів за поточним контролем.

Кількість балів	**Критерії оцінювання**
52–60	Систематичне відвідування лекцій та практичних занять, відсутність пропусків занять без поважної причини, відпрацювання тем практичних занять, пропущених з поважної причини, виконання завдань до кожного практичного заняття, висока активність роботи на практичному занятті, засвоєння всього обсягу матеріалу, повні та обґрунтовані відповіді при виконанні завдань, здатність визначення теоретичних питань, на які розраховані завдання, уміння сформувати своє ставлення до певної проблеми теми, вміння мислити абстрактно і узагальнено, здатність публічно представити матеріал.
44–51	Систематичне відвідування лекцій та практичних занять, відсутність пропусків занять без поважних причин, відпрацювання тем практичних занять, пропущених з поважної причини, виконання завдань до кожного практичного заняття, висока активність роботи на практичному занятті, засвоєння всього обсягу матеріалу, повні та обґрунтовані відповіді з несуттєвими помилками при виконанні завдань, здатність визначення теоретичних питань, на які розраховані завдання, уміння сформувати своє ставлення до певної проблеми теми, здатність публічно представити матеріал.
37–43	Наявність пропущених лекцій та практичних занять, відпрацювання тем пропущених практичних занять, виконання завдань до кожного практичного заняття, активна робота на практичних заняттях, засвоєння основних положень курсу, допущення декількох незначних помилок при виконанні завдань, здатність визначення теоретичних питань, на які розраховані завдання, здатність публічно представити матеріал.
29–36	Наявність пропущених лекцій та практичних занять, відпрацювання тем пропущених та практичних занять, епізодична відсутність виконання завдань, участь у роботі на практичних заняттях, засвоєння окремих положень

	матеріалу, неповні відповіді при виконанні завдань, складності при визначенні теоретичних питань, на які розраховані завдання, здатність публічно представити матеріал.
21–28	Несистематичне відвідування лекцій та практичних занять, відсутність на заняттях без поважних причин, наявність декількох невідпрацьованих тем пропущених практичних занять, епізодична відсутність виконаних завдань, участь у роботі на практичних заняттях, засвоєння окремих положень матеріалу тем змістовного розділу, неповні відповіді, допущення помилок при виконанні завдань, великі складності при визначенні теоретичних питань на які розраховані завдання, невпевнені навички публічного представлення матеріалу.
13-20	Епізодичне відвідування лекцій та практичних занять, відсутність на заняттях без поважної причини, наявність невідпрацьованих тем пропущених лекцій та практичних занять, епізодична відсутність виконаних завдань, пасивна робота на практичних заняттях (участь у роботі останніх лише за наявності стимулу з боку викладача), наявність певного уявлення щодо матеріалу тем змістовного розділу, неповні відповіді, допущення значної кількості помилок при виконання завдання, невміння визначити теоретичні питання, на які розраховано завдання, невпевнені навички публічного представлення матеріалу.
6-12	Систематичні пропуски лекцій та практичних занять без поважних причин, наявність невідпрацьованих тем пропущених лекцій та практичних занять, систематична відсутність виконаних завдань, пасивність у роботі на практичних заняттях, неповні, необґрунтовані відповіді, допущення істотних помилок при виконанні завдань, нездатність визначити теоретичні питання, на які розраховані завдання.
0-5	Систематичні пропуски лекцій та практичних занять без поважних причин, теми пропущених лекцій та практичних занять не відпрацьовані, систематична відсутність виконаних завдань, пасивність у роботі на практичних заняттях, відсутність знань, неповні, необґрунтовані відповіді, допущення істотних помилок при виконанні завдання, нездатність визначити теоретичні питання, на які розраховані завдання, невміння публічно представити матеріал, порушення норм академічної доброчесності при виконанні завдань.

Результати оцінювання роботи здобувачів фіксуються у відповідній відомості.

Здобувачі, які були відсутні на лекції чи практичному занятті або отримали незадовільну оцінку, відпрацьовують пропущене заняття або незадовільну оцінку викладачу у дні його консультацій за графіком, затвердженим кафедрою. Для відпрацювання здобувач зобов'язаний надати індивідуально виконане завдання за темою пропущеного заняття та продемонструвати належний рівень теоретичної підготовки за темою заняття, яке відпрацьовується.

До заліку допускаються здобувачі, які були присутніми не менш ніж на 70% занять з навчальної дисципліни, враховуючи відпрацьовані, та набрали не менш, ніж 25 балів за поточний контроль знань.

Оцінювання знань та умінь здобувачів при підсумковому контролі здійснюється відповідно до наступних критеріїв:

Кількість балів	**Критерії оцінювання**
40	Здобувач правильно відповів на всі тестові питання.
30	Здобувач правильно відповів на не менш, ніж 75 % тестових питань.

20	Здобувач правильно відповів на не менш, ніж 50 % тестових питань.
10	Здобувач правильно відповів на не менш ніж 25 % тестових питань.
0	Здобувач не відповів на жодне з тестових питань.
Правильна відповідь на одне тестове питання – 1 бал.	

Шкала оцінювання

Сума балів за всі види навчальної діяльності протягом семестру	Оцінка	
	для чотирирівневої шкали оцінювання	для дворівневої шкали оцінювання
90–100	відмінно	зараховано
70–89	добре	
50–69	задовільно	
1–49	незадовільно	не зараховано

КАЛЕНДАР КУРСУ
«Міжнародна інформаційна безпека»

№ тижня (дні тижня)	Тема	Форми організації навчання	Кількість годин	Завдання для самостійної роботи
1 семестр 2020 / 2021 навчального року				
1	Концепція інформаційного протиборства в міжнародних відносинах.	Лекція	2	1. Ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття.
2	Теоретичні засади інформаційної безпеки.	Лекція	2	1. Ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття.
3	Концепція інформаційного протиборства в міжнародних відносинах.	Практичне заняття	2	1. Підготувати презентації доповідей з визначених тем (на вибір). 2. Підготувати тематичну схему. 3. Ознайомитися та

				проаналізувати наукову статтю. 4. Підготувати есе на визначену тему.
4	Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру.	Лекція	2	1. Ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття.
5	Теоретичні засади інформаційної безпеки.	Практичне заняття	2	1. Підготувати презентації доповідей з визначених тем (на вибір). 2. Підготувати тематичну схему. 3. Підготувати есе на визначену тему (на вибір).
6	Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки.	Лекція	2	1. Ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття.
7	Інституційно-правові засади інформаційної безпеки у глобальній системі підтримання миру.	Практичне заняття	2	1. Підготувати презентації доповідей з визначених тем (на вибір). 2. Підготувати тематичну схему. 3. Підготувати есе на визначену тему (на вибір).
8	Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки.	Лекція	2	1. Ознайомитися з лекційним матеріалом та з рекомендованою літературою за темою та бути готовими відповідати на усні запитання за навчальними питаннями практичного заняття.
9	Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки.	Практичне заняття	2	1. Підготувати презентації доповідей з визначених тем (на вибір). 2. Ознайомитися та проаналізувати нормативний акт.

				3. Підготувати тематичну схему.
10	Інструменти регіонального співробітництва у сфері міжнародної інформаційної безпеки.	Практичне заняття	2	1. Підготувати презентації доповідей з визначених тем (на вибір). 2. Ознайомитися та проаналізувати нормативний акт. 3. Поділитися на дві групи та підготувати питання здобувачам іншої групи за всіма темами курсу для колоквіуму
18–20	Підсумковий семестровий контроль			1. Підготуватися до тестових завдань за запропонованим переліком питань для підготовки.