МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДВНЗ «ПРИКАРПАТСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТЕФАНИКА»

Факультет історії, політології і міжнародних відносин

Кафедра міжнародних економічних відносин

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Кібер-безпека в міжнародному бізнесі

Освітня програма «Управління міжнародним бізнесом»

Спеціальність 073 «Менеджмент»

Галузь знань 07 «Управління та адміністрування»

Затверджено на
засіданні кафедри
міжнародних економічних
відносин
Протокол № 1 від «29» серпня 2022 р.

м.Івано-Франківськ– 2022

ЗМІСТ

1. Загальна інформація

Назва дисципліни	Кібер-безпека в міжнародному бізнесі
Освітня програма	Управління міжнародним бізнесом
Спеціалізація (за наявності)	
Спеціальність	073 «Менеджмент»
Галузь знань	07 Управління і адміністрування
Освітній рівень	бакалавр
Статус дисципліни	Обов'язкова дисципліна
Курс/семестр	4/7
Розподіл за видами занять та годинами навчання (якщо передбачені інші види, додати)	Лекції – 12год. Практичні заняття – 18 год. Самостійна робота – 60 год.
Мова викладання	українська
Посилання на сайт дистанційного навчання	https://d-learn.pro/

2. Описдисципліни

Мета та цілі дисципліни
Мета дисципліни є формування системи теоретичних знань і практичних навичок до розуміння закономірностей місця і ролі кібербезпеки у міжнародному бізнесі, а також особливостей застосуванню методів та засобів ефективного та безпекового поводження з інформацією в умовах широкого використання сучасних інформаційних технологій. Основними **завданнями** вивчення студентами дисципліни «Кібер-безпека в міжнародному бізнесі» є: – забезпечити теоретичний та емпіричний підхід до розуміння сутності «кібербезпека», «кіберзлочинності» та «кібертероризму» в міжнародному бізнесі; – надати знання щодо міжнародних правових інструментів і механізмів протидії інформаційним порушенням та кіберзлочинності; – знати основи міжнародної політики у сфері забезпечення інформаційної безпеки та зміст основних положень нормативно-правових актів у сфері інформаційної безпеки; – сформувати систему спеціальних теоретичних знань нормативно-правового забезпечення для збереження комерційної та державної інформації; – сформувати знання про значущість особливостей організації допуску та доступу персоналу до конфіденційної інформації в міжнародному бізнесі; – розкрити сутність захисту професійної таємниці та персональних даних в міжнародному бізнесі.
Компетентності
ЗК9. Здатність вчитися і оволодівати сучасними знаннями. ЗК11. Здатність до адаптації та дії в новій ситуації. СК17. Здатність використовувати професійно-комунікативні навики для представлення, обґрунтування та відстоювання економічних інтересів суб'єктів міжнародного бізнесу та реалізовувати їх в умовах цифрової економіки, логістики, інформаційних технологій.
Програмні результати навчання
ПРН 16. Демонструвати навички самостійної роботи, гнучкого мислення, відкритості до нових знань, бути критичним і самокритичним. ПРН 19. Організовувати та здійснювати ефективні комунікації з представниками міжнародного бізнесу іноземною мовою в.т.ч через використання on-line платформ зв'язку та передачі даних.

3. Структура дисципліни

№ з/п	Тема	Результати навчання	Завдання
1	**Тема 1.** Характеристика стандартів із забезпечення кібербезпеки в міжнародному	• Розглянути сутністно-змістовну характеристику ефективних стандартів з кібербезпеки в міжнародному бізнесі;	• Тести, • Контрольні запитання, • Кейси, • Завдання для індивідуальної роботи, • Завдання для самостійної

	бізнесі	• Проаналізувати корисність та актуальність стандартів, а також форми представлення стандартів в міжнародному бізнесі. • Засвоїти поняття нормативно-правовий базис у сфері міжнародного бізнесу.	роботи
2	**Тема 2.** Інформаційна безпека як об'єкт правовідносин	• Ознайомитися із поняттями «суспільні відносини» та «правовідносини»; • Проаналізувати та систематизувати отриману інформацію щодо взаємозв`язоків інформаційної безпеки з правовідносинами у системі міжнародного бізнесу; • Проаналізувати причини загроз прямого впливу на інформаційну безпеку міжнародного бізнесу.	• Тести, • Контрольні запитання, • Кейси, • Завдання для індивідуальної роботи, • Завдання для самостійної роботи
3	**Тема 3.** Поняття кібербезпеки, кіберзлочинності та кібертероризму в різних країнах.	• Засвоїти розуміння понятійно-категоріального апарату «кібернетична безпека» (кібербезпека); • Розглянути вплив стратегії кібербезпеки України та на міжнародного простору. • Визначити можливості упорядковування отриманої інформації щодо конвенції про кіберзлочинність та кібертероризм.	• Тести, • Контрольні запитання, • Кейси, • Завдання для індивідуальної роботи, • Завдання для самостійної роботи
4	**Тема 4.** Міжнародні правові інструменти і механізми протидії інформаційним порушенням та	• Засвоїти особливості змістовно-типологічної характеристики національних стратегій кібербезпеки різних країн;	• Тести, • Контрольні запитання, • Кейси, • Завдання для індивідуальної роботи, • Завдання для самостійної роботи

	кіберзлочинності	• Засвоїти особливості функціонування стратегії кібербезпеки США та Європейського Союзу; • Проаналізувати конвенцію про кіберзлочинність.	
5	**Тема 5.** Нормативно-правове забезпечення для збереження комерційної та державної інформації	• Засвоїти та упорядковувати отриману інформацію щодо відомостей до комерційної таємниці та державної таємниці. • Набути вмінь до оцінки результатів збереження комерційної таємниці у міжнародному бізнесі; • Зосвоїти особливості формування перспективних пріоритетів розвитку комерційної таємниці міжнародних компаній.	• Тести, • Контрольні запитання, • Кейси, • Завдання для індивідуальної роботи, • Завдання для самостійної роботи
6	**Тема 6.** Організація допуску та доступу персоналу до конфіденційної інформації в міжнародному бізнесі	• Проаналізувати організацію доступу до таємної інформації міжнародних фірм; • З'ясувати особливості захисту службової інформації міжнародних компаній; • Окреслити основні напрями захисту електронної інформації в міжнародному бізнесі.	• Тести, • Контрольні запитання, • Кейси, • Завдання для індивідуальної роботи, • Завдання для самостійної роботи
7	**Тема 7.** Захист професійної таємниці та персональних даних в міжнародному бізнесі	• Дослідити та упорядковувати отриману інформацію щодо відомостей до захисту професійної таємниці та персональних даних (інформації про особу) у сфері міжнародного бізнесу; • Обгрунтувати основні способи протидії загрозам витоку інформації про особисті дані працівників	• Тести, • Контрольні запитання, • Кейси, • Завдання для індивідуальної роботи, • Завдання для самостійної роботи

		міжнародної компанії; • Охарактеризувати інноваційні методики захисту персональних даних міжнародних компаній в умовах сучасних викликів.	
8	**Тема 8.** Організаційна робота із захисту інформації з обмеженим доступом в країнах НАТО і ЄС	• Дослідити міжнародний стандарт безпеки ISO/IEC 17799; • Обгрунтувати основні п'ять інституційних принципів, покликаних забезпечити високий рівень інформаційної безпеки; • Охарактеризувати принципи та мінімальні стандарти політики безпеки країн ЄС; • З'ясувати особливості норм поводження з несекретною інформацією НАТО.	• Тести, • Контрольні запитання, • Кейси, • Завдання для індивідуальної роботи, • Завдання для самостійної роботи

4. Система оцінювання курсу

Накопичування балів під час вивчення дисципліни	
Види навчальної роботи	Максимальна кількість балів
Семінарські заняття	40
Бали за теми, винесені на лекційні заняття	30
Бали за індивідуальну роботу	20
Бали за самостійне опрацювання додаткової літератури	10
Максимальна кількість балів	100

5. Оцінювання відповідно до графіку навчального процесу

Робота на парах	Оцінка за контрольну роботу	Оцінка за індивідуальну роботу	Оцінка за самостійну роботу	**Разом**
40	30	20	10	**100**
• Оцінювання відповідей студентів на практичних заняттях відбувається за 100 бальною шкалою				

Поточний контроль з дисципліни «Кібер-безпека в міжнародному бізнесі» відбувається шляхом перевірки засвоєння студентами знань та умінь в ході семінарських занять, написання контрольної роботи, підготовки індивідуальної роботи та контролю самостійного опрацьованої додаткової літератури.

Перевірка засвоєння студентами знань та умінь в ході семінарських занять здійснюється шляхом оцінювання усних відповідей (в тому числі у формі презентацій), коротких письмових / тестових робіт. За опрацювання тем, визначених для семінарських занять студент може отримати максимально 40 балів. Відповідна форма активності студентів оцінюється за стобальною системою. У кінці семестру сума всіх оцінок ділиться на кількість оцінок, далі вона ділиться на 10 та множиться на 4.

Контроль засвоєння знань та навичок, що базуються на лекційному матеріалі, здійснюється шляхом написання студентами контрольної роботи (у розгорнутій та/або тестовій формі). За опрацювання тем, визначених для семінарських занять, студент може отримати максимально 30 балів.

Навики роботи із науковою літературою, вміння аналізувати знайдені матеріали, робити висновки та узагальнення студенти реалізують шляхом написання індивідуальних робіт. Індивідуальна робота оцінюється максимально у 20 балів.

Студентам також пропонується самостійне опрацювання наукових джерел, які є знаковими для відповідної дисципліни. Контроль засвоєння відповідних знань здійснюється у тестовій формі та максимально оцінюється у 10 балів.

Семестровий контроль у формі заліку передбачає, що підсумкова оцінка з навчальної дисципліни визначається як сума оцінок за поточний контроль знань.

Критерії поточного оцінювання:

Відповідно до *Положення про порядок організації та проведення оцінювання успішності здобувачів вищої освіти ДВНЗ «Прикарпатського національного університету*

ім. Василя Стефаника» (введено в дію наказом ректора № 799 від 26.11.2019 р.; із внесеними змінами наказом № 212 від 06.04.2021 р.) та *Положення про організацію освітнього процесу та розробку основних документів з організації освітнього процесу в ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»* (Нова редакція) (введено в дію наказом ректора № 361 від 31.07.2020 р.) знання оцінюються як з теоретичної, так і з практичної підготовки відповідно до національної шкали за такими критеріями:

- «відмінно» – здобувач освіти міцно засвоїв теоретичний матеріал, глибоко і всебічно знає зміст навчальної дисципліни, основні положення наукових першоджерел та рекомендованої літератури, логічно мислить і будує відповідь, вільно використовує набуті теоретичні знання при аналізі практичного матеріалу, висловлює своє ставлення до тих чи інших проблем, демонструє високий рівень засвоєння практичних навичок;
- «добре» – здобувач освіти добре засвоїв теоретичний матеріал, володіє основними аспектами з першоджерел та рекомендованої літератури, аргументовано викладає його; має практичні навички, висловлює свої міркування з приводу тих чи інших проблем, але припускається певних неточностей і похибок у логіці викладу теоретичного змісту або при аналізі практичного матеріалу;
- «задовільно» – здобувач освіти в основному опанував теоретичними знаннями навчальної дисципліни, орієнтується в першоджерелах та рекомендованій літературі, але непереконливо відповідає, плутає поняття, додаткові питання викликають невпевненість або відсутність стабільних знань; відповідаючи на запитання практичного характеру, виявляє неточності у знаннях, не вміє оцінювати факти та явища, пов'язувати їх із майбутньою діяльністю;
- «незадовільно» – здобувач освіти не опанував навчальний матеріал дисципліни, не знає наукових фактів, визначень, майже не орієнтується в першоджерелах та рекомендованій літературі, відсутні наукове мислення, практичні навички не сформовані.

6. Ресурсне забезпечення

Матеріально-технічне забезпечення	Мультимедіа (відеофайли, рисунки, схеми)

Література:

Основна

1. Бурячок В.Л., Гулак Г.М., Толубко В.Б. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби: підручник. К.: ДУТ. 2019. 449 с.
2. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: монографія. Житомир: ЖНАЕУ. 2019. 636 с.
3. Довгань О.Д. Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти: монографія; НАПрН України, НДІІП, НАН України, Нац. б-ка ім. В.І. Вернадського. Київ. 2018. 388 с.
4. Вівчар О. І., Зайцева-Калаур І. В., Зяйлик М. Ф. Нормативно-правові аспекти міжнародного співробітництва: безпекознавчі контексти. Український журнал прикладної економіки. 2021. № 2. С. 119–124.
5. Вівчар О. І. Асиметрична стратегія як вектор зміцнення міжнародної стратегії. Звітна наукова конференція викладачів, докторантів, аспірантів університету Прикарпатський національний університет ім. В. Стефаника. 04–08 квітня 2022. Івано-Франківськ. С. 50-53.
6. Інформаційна безпека : підручник ; за аг. ред.. В.В. Остроухова. К. : ДНУ «Книжкова палата Україна». 2019. 264 с.
7. Параметри оцінки ефективності інформаційного права ; за ред. П.В. Кіндрат. Право і суспільство. 2016. № 5. С. 102–107. ISSN 2078–3736
8. ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT).
9. ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT).

10. Інформаційна та кібербезпека: соціотехнічний аспект: підручник ; за заг. ред. д-ра техн. наук, професора В.Б. Толубка. К.: ДУТ. 2018. 288 с.
11. Чудик Н. Міжнародний бізнес. К.: Вектор. 2018. 410 с.

Додаткова

1. Харарі Ювал Ной. 21 урок для 21 століття / Ювал Ной Харарі; пер. з англ. О. Дем`янчука.Київ: Форс Україна. 2018. 416 с.
2. Чухно А.А. Інституціонально-інформаційна економіка: підручник.К.:Знання. 2018. 687 с.
3. Cabric M. Corporate Security Management. Challenges, Risks, and Strategies. 2015. URL: https://dl.acm.org/doi/pdf/10.5555/2843502
4. Drobyazko S., Alieksieienko I., Kobets M., Kiselyova E., Lohvynenko M. Transnationalisation and segment security of the international labor market. Journal of "Security and sustainability issues". December Volume 9 Number 2. 2019. URL: https://jssidoi.org/jssi/uploads/papers/34/Drobyazko_Transnationalisation_and_segment_security_of_the_international_labor_market.pdf
5. Farion A., Dluhopolskyi O., Banakh S., Moskaliuk N., Farion M. and Ivashuk Y. Using Blockchain Technology for Boost Cyber Security. International Conference "Advanced Computer Information Technologies". University of South Bohemia. Czech Republic. ACIT'2019. P. 452–455. URL: https://ieeexplore.ieee.org/document/8780019
6. Food and Agriculture Organization of the United Nations. «The State of Food Security and Nutrition in the World 2019» Safeguarding against economic slowdowns and downturns. Rome, FAO. URL: http://www.fao.org/3/ca5162en/ca5162en.pdf
7. Halibozek E., Kovacich G. The Manager's Handbook for Corporate Security: Establishing and Managing Assets Protection Program. Second edition. April 2017. URL: https://books.google.com.ua/books?id=qDKQDQAAQBAJ&pg=PA420&lpg=PA420&dq=corporate+security+articles&source=bl&ots=D1xJJ_JAnj&sig=ACfU3U0IN16dyEtmQy-Q65-9jgWCx-0sCg&hl=uk&sa=X&ved=2ahUKEwj9s9qUr_zpAhVnxIsKHbwRCesQ6AEwCXoECAoQAQ#v=onepage&q=corporate%20secur&f=false
8. Hryhoruk P. M., Khrushch N. A., Chuniak O. V. Conception of modeling the system of ensuring financial economic security. Scientific Bulletin of Polissia. 2019. Vol. 17. Issue 1. P. 158–165.
9. Liber D. Do's and Don'ts: Security Management in a Growing Company. 2015. URL: http://securityintelligence.com
10. Redkva O., Shatarskyi A. Organizational and legal foundations of the impact of criminal activity on the economic security of business structures in transformational conditions. Vector European : Revista ştiinţifico-practică. Universitatea de studii europene din Moldova. Chișinău. Nr 2 2021. P. 87–93.
11. Krzywkowska J. Rules of functioning of roman catholic parishes in Poland during the epidemic. State and society facing pandemic. Edited by Eduard Burda, Carmen Lazaro Guillamon, Magdalena Sitek. Bratislava : Wolters Kluwer. 2020. P. 439–450.
12. Stifel M. Securing the modern economy: Transforming cybersecurity through sustainability. Megan Stifel. Public Knowledge, April 2018. URL: https://www.publicknowledge.org/assets/uploads/documents/Securing_the_Modern_Economy--Transforming_Cybersecurity_Through_Sustainability_FINAL_4.18.18_PK.pdf\
13. Vivchar O., Gevko V., Zaitseva-Kalaur I., Redkva O. Organizational and legal procedures for ensuring the security and protection of economic entity: a security rnowledgeable approach. Studia Prawnoustrojove. Wydawnictwo Uniwersytetu Warmińsko–Mazurskiego w Olsztynie 46. 2019. P. 453–464.
14. Vivchar O., Gevko V., Redkva O. Investigation of the methodological contexts contexts for systematic assessment of entrepreneurial structures: a safe measurement of the regional approach. Vector European : Revista ştiințifico-practică. Universitatea de studii europene din Moldova. Chișinău. Nr 2. 2020. P. 129–136.
15. Vivchar O., Muravska Y. NATO-UKRAINE COOPERATION AS AN IMPORTANT MECHANISM FOR COUNTERACTING HYBRID WARFARE / NATIONAL SECURITY IN MODERN WORLD. LEGAL, TECHNOLOGICAL AND SOCIAL COMMUNICATION ASPECTS: collective monograph; ed.: Jacek Mrozek, Serhiy Banakh, Svitlana Mazepa. Publisher: centre for Eastern Europe Research UWM in Olsztyn. 2021. C. 73–80.

Ресурси курсу

Інформація про курс розміщена на сайті дистанційного навчання Прикарпатського національного університету імені Василя Стефаника

https://d-learn.pro/

7. Контактна інформація

Кафедра	Кафедра міжнародних відносин м. Івано-Франківськ, вул. Чорновола, 1, каб. 104. Тел.: +80342 75-20-27 Email: https://kmev.pnu.edu.ua/ Ст. лаборант кафедри: Грушко Оксана Дмитрівна Сторінки в соцмережах: https://www.facebook.com/groups/2021045604705063
Викладач	 Вівчар Оксана Іванівна доктор економічних наук, професор
Контактна інформація викладача	+80342 75-20-27 oksana.vivchar@pnu.edu.ua

8. Політика навчальної дисципліни

Академічна доброчесність	Дотримання академічної доброчесності засновується наряді положень та принципів академічної доброчесності, що регламентують діяльність здобувачів вищої освіти та викладачівуніверситету. Ознайомитися з даними положеннями та документами можна за посиланням: https://pnu.edu.ua/положення-про-запобігання-плагіату/
Пропуски занять (відпрацювання)	Можливість і порядок відпрацювання пропущених здобувачем освіти занять регламентується *Положення про порядок організації та проведення оцінювання успішності здобувачів освіти ДВНЗ «Прикарпатського національного університету ім. Василя Стефаника»* (введено в дію наказом ректора № 799 від 26.11.2019 р.; із внесеними змінами наказом № 212 від 06.04.2021 р.).
Виконання завдання пізніше встановленого терміну	У разі виконання завдання здобувачем освіти пізніше встановленого терміну, без попереднього узгодження ситуації з викладачем, оцінка за завдання – «незадовільно», відповідно до *Положення про порядок організації та проведення оцінювання успішності студентів ДВНЗ «Прикарпатського національного університету ім. Василя Стефаника»* (введено в дію наказом ректора № 799 від 26.11.2019 р.; із внесеними змінами наказом № 212 від 06.04.2021 р.).
Невідповідна поведінка під час заняття	Невідповідна поведінка під час заняття Невідповідна поведінка під час заняття регламентується рядом положень про академічну доброчесність та може призвести до відрахування здобувача вищої освіти «за порушення навчальної дисципліни і правил внутрішнього розпорядку вищого закладу освіти», відповідно до *Положення про порядок переведення, відрахування та поновлення студентів вищих закладів освіти»* (затверджене наказом Міністерства України № 245 від 15.07.1996 р.).
Додаткові бали	Студент має змогу також отримати **додаткові бали**, пройшовши

	навчальний курс у вигляді неформальної освіти з отриманням сертифікату в межах тематики дисципліни впродовж навчального семестру; взявши участь у науковому, освітньому чи прикладному проєкті, конференції, круглому столі, інших видах наукової активності, які відповідають профілю дисципліни; опублікувавши наукову працю, яка відповідає профілю дисципліни. Відповідно до *Положення про порядок організації та проведення оцінювання успішності студентів ДВНЗ «Прикарпатського національного університету ім. Василя Стефаника»* (введено в дію наказом ректора № 799 від 26.11.2019 р.; із внесеними змінами наказом № 212 від 06.04.2021 р.). відповідні студенти можуть отримати додаткові бали на підставі рішенням кафедри міжнародних відносин.
Неформальна освіта	Можливість зарахування результатів неформальної освіти регламентується *Положенням про порядок зарахування результатів неформальної освіти у ДВНЗ «Прикарпатський національний університет імені Василя Стефаника»* (введено в дію наказом ректора № 819 від 29.11.2019; із внесеними змінами наказом № 80 від 12.02.2021 р.).

Викладач Вівчар О.І.