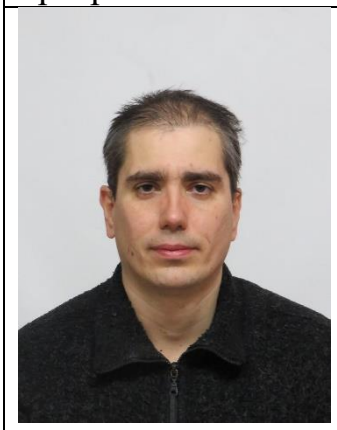
ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
СИСТЕМА УПРАВЛІННЯ ЯКІСТЮ
Система забезпечення якості освітньої діяльності та якості вищої освіти
сертифікована на відповідність ДСТУ ISO 9001:2015 / ISO 9001:2015
Кафедра інженерії програмного забезпечення та кібербезпеки

ОСНОВИ КІБЕРДИПЛОМАТІЇ АНГЛІЙСЬКОЮ МОВОЮ /
THE BASICS OF CYBER DIPLOMACY IN ENGLISH

СИЛАБУС/
SILABUS

ЗАТВЕРДЖЕНО
засіданням кафедри
(протокол №. 1
від «04» серпня 2024 р.)
завідувач кафедри
_____ Олена КРИВОРУЧКО

Київ 2024

Назва освітньої компоненти	**ОСНОВИ КІБЕРДИПЛОМАТІЇ АНГЛІЙСЬКОЮ МОВОЮ /** THE BASICS OF CYBER DIPLOMACY IN ENGLISH
Спеціальність	125 «Кібербезпека та захист інформації»
Освітній ступінь	Другий (магістерський)
Освітньо-професійна програма	**БЕЗПЕКА СИСТЕМ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ В ЕКОНОМІЦІ**
	Лектор: **Токар Володимир** -професор кафедри інженерії програмного забезпечення та кібербезпеки -доктор економічних наук -професор Резюме викладача: https://knute.edu.ua/blog/read/?pid=43230&uk Науковий профіль: https://orcid.org/0000-0002-1879-5855 е-пошта: v.tokar@knute.edu.ua
	Асистент лектора: **Гайдук Олег** - Старший викладач - перший заступник Голови Громадської спілки КіберКовчег. - учасник Громадської ради Мінцифри. - голова Ради з інформаційної та кібербезпеки України, утвореної Меморандумом РНБО, Мінцифри та Держспецзв'язку України Резюме викладача: https://knute.edu.ua/blog/read/?pid=46833&uk е-пошта: o.hayduk@knute.edu.ua
Консультації	https://knute.edu.ua/blog/read/?pid=47103&uk
Програма освітньої компоненти	https://knute.edu.ua/blog/read/?pid=48216
ЗМІСТ ОСВІТНЬОЇ КОМПОНЕНТИ	
Тема 1. Кібердипломатія: походження, розвиток, основні принципи, вплив на міжнародні	Концепція і стратегія кібердипломатії. Походження та історія. Кібердипломатія як інструмент вирішення конфліктів. Основні аспекти міжнародних норм та правил у сфері кібербезпеки. Традиційні дипломатичні методи і практики, їх трансформація в кіберпросторі. Парадигма захисту національних інтересів в кіберпросторі. Просування свободи слова, приватності та інших прав людини в кіберпросторі.

відносини та політику	Вплив кібердипломатії на міжнародну політику. Інструментарій кібердипломатії. Порівняння підходів та стратегій.
Тема 2. Публічна дипломатія, Цифрова дипломатія, Дипломатія швидкого реагування	Комунікаційні стратегії. Вплив на громадську думку. Використання цифрових інструментів і платформ для ефективної дипломатичної діяльності, включаючи соціальні мережі, онлайн-кампанії та цифрові комунікаційні стратегії. Інструменти своєчасної та ефективної дипломатичної реакції на міжнародні кризи та надзвичайні ситуації.
Тема 3. Технологічна дипломатія	Історія міжнародних відносин щодо обмеження та нерозповсюдження технологій. Вплив технологій на розвиток дипломатії. Кур'єри. Шифрування. Тегграф. Телетайп. Електрона пошта. Месенджери. Електронне урядування. Міжнародні переговори. Економічна дипломатія. Правові та етичні питання в ІКТ. Технологічні інновації та їх вплив на дипломатію. Стратегічне планування в дипломатії. Управління ризиками в дипломатії. Методи та інструменти для аналізу та прогнозування тенденцій в сфері ІКТ. Міжнародні стандарти в сфері ІКТ. Міжнародні експертні групи.
Тема 4. Підхід міжнародних організацій до розвитку кіберсфери та ІКТ. Регулювання відносин країн в кіберпросторі	ООН, ЄС, НАТО, ОБСЄ, МТС ITU та інші. Суверенітет, неприпустимість втручання у внутрішні справи, мирне співіснування. Міжнародна співпраця в сфері кібербезпеки, ініціативи, організації та угоди. Міжнародні угоди та договори у сфері кіберпростору. Особлива роль кібердипломатії міжнародних організацій у врегулюванні конфліктів у кіберпросторі, основні механізми та процедури. Відповідальна поведінка держав та принципи ООН. Етичні норми ООН. ООН: історія питання від першої відкритої робочої групи до глобальної цифрової угоди. 17 цілей ООН. 11 норм відповідальної поведінки в кіберпросторі.
Тема 5. Міжнародне право в кіберпросторі, виклики, проблеми та потенційні рішення. Міжнародне цивільне право	Історія і сучасні виклики. Суверенітет, юрисдикція та принципи. Проблеми міжнародного права в кіберпросторі, конфіденційність, свобода вираження поглядів та відповідальність держав. Потенційні рішення для міжнародного права в кіберпросторі, розвиток нових норм, вдосконалення існуючих договорів та угод. Визначення агресії, пропорційність заходів самозахисту та права на самооборону. Кібершпигунство та міжнародне право, порушення суверенітету, недоторканність приватного життя та захист державної і комерційної таємниць. Роль недержавних суб`єктів у врегулюванні конфліктів в кіберпросторі.

Тема 6. Кібербезпека та кіберзахист: технічні, організаційні і правові основи	Сучасні технології і методи для захисту інформаційних систем та мереж. Антивіруси. Брандмауери. Шифрування даних. Криптографія. Аутентифікація. Політики кібербезпеки та адміністративно-організаційні процедури. Поняття внутрішньодержавного механізму кібербезпеки та кіберзахисту. Загальносвітові основні принципи регулювання кібербезпеки, захисту персональних даних та захисту інтелектуальної власності. Національна система кібербезпеки та внутрішньодержавний механізм кібербезпеки в Україні.
Тема 7. Стандарти інформаційної та кібербезпеки в Україні та світі	Основи національних стандартів, державні вимоги та регулювання. ISO/IEC 27000, NIST Cybersecurity Framework, COBIT. Роль міжнародних організацій у розробці та впровадженні стандартів інформаційної та кібербезпеки, ISO, IEC, ITU. Керування ризиками в інформаційній та кібербезпеці, методи оцінки ризиків, управління ризиками та мінімізація ризиків. Захист даних та приватності, GDPR, CCPA, HIPAA. Безпека програмного забезпечення та мереж, OWASP, NIST SP 800-53, CIS Controls. Безпека хмарних обчислень, CSA CCM, NIST SP 800-144, ISO/IEC 27017. Інцидент-менеджмент та відновлення після інциденту, NIST SP 800-61, ISO/IEC 27035, SANS Incident Response Process. Стандарти кібербезпеки для критичної інфраструктури: NERC CIP, NIST SP 800-82, IEC 62443.
Тема 8. Кіберконфлікти та кібервійни: політичні, юридичні та етичні аспекти	Основи політичних процесів в демократичних державах. Існуючі політики виборів, референдумів і інших волевиявлень людей. Концепція кіберконфлікту та кібервійни. Поняття гібридної війни. Виклики для міжнародного права. Агресії оборона в кіберпросторі. Відповідальність за кібератаки та захист прав людини. Етика використання технологій для досягнення політичних цілей. Парадигма втручання у внутрішні справи держав. Досвід США та ЄС
Тема 9. Кібертероризм та кібершпигунство: визначення, організаційні основи боротьби, методи та протидія. Протидія розвідкам в кіберпросторі	Визначення та організаційні основи. Методи та протидія. Міжнародна співпраця та правові рамки для боротьби з кібертероризмом і кібершпигунством в світі. Етичні міркування та права людини при розслідуванні кібертероризму і кібершпигунства. Державно-приватне партнерство в боротьбі з кібертероризмом і кібершпигунством. Майбутні тенденції та виклики. Аналіз випадків: розгляд прикладів.
Тема 10. Законодавче регулювання ІТ та кібербезпеки,	Регулювання ІТ та кібербезпеки в Україні, законодавчі акти, стандарти та ініціативи. Регулювання ІТ та кібербезпеки в країнах Європи, ЄС, Великобританія, Німеччина, Франція та інші. Регулювання ІТ та кібербезпеки в країнах Америки:

кіберзахисту та кібероборони в Україні, в країнах Європи та Америки, в Азії та країнах Африки	США, Канада, Бразилія та інші. Регулювання ІТ та кібербезпеки в країнах Азії: Китай, Японія, Індія та інші. Регулювання ІТ та кібербезпеки в країнах Африки: Південна Африка, Нігерія, Кенія та інші. Угоди та договори у сфері ІТ та кібербезпеки. Роль недержавних суб'єктів у регулюванні ІТ та кібербезпеки, громадські організації, приватні підприємства та академічні кола. Тенденції та виклики регулювання ІТ та кібербезпеки, штучний інтелект, Інтернет речей, 5G та інші. Розвиток національних стратегій кібербезпеки та їх вплив на регулювання ІТ та кібербезпеки.
Тема 11. Кібердіалог	Коцепція кібердіадогу. Дискусії та обмін інформацією в кібердіазозі. Методологія розробки спільних підходів до викликів та можливостей, пов'язаних з ІКТ. Побудова довіри між учасниками. Розвиток міжнародних норм і правил у сфері кібербезпеки. Рівні кібердіалогу. Двосторонні, регіональні та багатосторонні сфери кібердіалогу. Кібердіалог як рамка двосторонніх відносин в кіберсфері.
Тема 12. Організаційні основи, національні і внутрішньодержавні механізми реагування на кіберінциденти, порівняльний аналіз організації кібербезпеки та кіберзахисту в світі	Державні органи, закони та регуляторні акти в сфері кібербезпеки в країнах Європи, Північної Америки та Азії. Особливості організаційних основ кібербезпеки, стратегій і політик, внутрішньодержавні механізми, порівняльний аналіз та тенденції. Основи міжнародної співпраці в сфері кібербезпеки. Тенденції взаємодії державних органів з приватним сектором та громадськістю. Роль недержавних суб'єктів у забезпеченні кібербезпеки.
Тема 13. Основи ІПСО та базові аспекти протидії дезінформації. ОСІНТ в кіберпросторі	Основи Інформаційно-психологічного забезпечення операцій (ІПСО), їх визначення, цілі та методи. Базові аспекти протидії дезінформації, методи та інструменти. OSINT (Операції інформаційного впливу) в кіберпросторі, їх визначення, цілі та методи. ІПСО та OSINT у контексті міжнародної безпеки та стабільності. Міжнародна співпраця у боротьбі з дезінформацією та OSINT. Роль недержавних суб'єктів у протидії дезінформації та OSINT. Регуляторне середовище для протидії дезінформації та Осінт, національні та міжнародні норми, стандарти та закони. Кібердипломатія та її роль у протидії дезінформації та OSINT.
Тема 14. Основи штучного інтелекту. Поняття квантових	Визначення штучного інтелекту (ШІ), історія, концепції та архітектури. Застосування ШІ у кібердипломатії, аналіз даних, прогнозування, автоматизація процесів. Етичні та правові аспекти ШІ в кібердипломатії, приватність, відповідальність, прозорість. ШІ та безпека кіберпростору, виявлення та

обчислень. Мережі контактних точок.	запобігання кібератакам, кібербезпека ШІ-систем. ШІ та дипломатичні переговори, моделювання сценаріїв, аналіз позицій та прогнозування результатів. ШІ та міжнародне право, аналіз та інтерпретація договорів, визначення юрисдикцій. ШІ та кібербезпека критичної інфраструктури, моніторинг, виявлення вразливостей та запобігання інцидентам. ШІ та протидія дезінформації, виявлення фейкових новин, фактчекінг та боротьба з OSINT. ШІ та кібердипломатія в контексті міжнародної безпеки та стабільності: виклики, проблеми та потенційні рішення. Освіта та навчання у сфері ШІ.

СПИСОК ОСНОВНИХ РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Cyberdiplomacy: Managing Security and Governance Online: навчальний посібник/, Shaun Riordan. Language: English. Видавництво Polity, 2019. -160 с.
2. Дипломатія: теорія, історія, практика: підручник /В.Г. Ціватий. Київ: Дип. акад. України при МЗС України, 2016. 396 с.
3. Теорія міжнародного права : навчально-методичний посібник / за ред. О. В. Бігняка. – Херсон : Гельветика, 2020. – 224 с.
4. Даник Ю.Г. Основи кібербезпеки та кібероборони: підручник / Ю.Г. Даник, П.П. Воробієнко, В.М. Чернега. – [Видання друге, перероб. та доп.]. – Одеса.: ОНАЗ ім. О.С. Попова, 2019. − 320 с. ISBN 978-617-582-069-8
5. Гребенюк А.М. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. – 144 с.

РЕЗУЛЬТАТИ ВИВЧЕННЯ ОСВІТНЬОЇ КОМПОНЕНТИ

Дисципліна забезпечує оволодіння здобувачами вищої освіти загальними та фаховими компетентностями і досягнення ними програмних результатів навчання:

КЗ-01.	Здатність застосовувати знання у практичних ситуаціях.
КЗ- 03.	Здатність проводити дослідження на відповідному рівні.
КЗ- 05.	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КЗ- 06.	Здатність діяти соціально відповідально та громадсько свідомо
КЗ- 07.	Здатність до адаптації та дії у новій ситуації.
КЗ- 08.	Здатність до вибору стратегії спілкування, працювати в команді.
КЗ- 09.	Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися іноземною мовою (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність.
КФ- 02.	Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і

	використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ- 04.	Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ- 05.	Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ- 10.	Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.
КФ- 12.	Здатність виконувати обов'язки внутрішнього консультанта і радника у своїй експертній області.
РН15.	Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
РН16.	Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень..
РН17.	Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
РН18.	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.
РН25.	*Виконувати обов'язки внутрішнього консультанта/ радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації.*
РН26.	*Комунікувати з керівниками різних рівнів (міжособистісне спілкування, доступність, уміння ефективно сприймати мову виступаючих, відповідно до аудиторії коректувати стиль і мову виступу).*

ОЦІНЮВАННЯ ЗНАНЬ ЗДОБУВАЧІВ ОСВІТИ

Сума балів, накопичених здобувачем вищої освіти за виконання всіх видів поточних навчальних завдань (робіт) на лабораторних/практичних заняттях, свідчить про ступінь оволодіння ним програмою освітньої компоненти на конкретному етапі її вивчення. Протягом семестру здобувачі освіти можуть набрати від 0 до 100 балів,

що переводяться у національну шкалу оцінювання і відповідно у шкалу ЄКТС. Кількість балів відповідає певному рівню засвоєння дисципліни

Довідник з розподілу оцінок ДТЕУ (Шкала ЄКТС):

Бали ДТЕУ	Відсоток балів відносно загальної кількості одержаних прохідних балів	Кумулятивний відсоток отриманих прохідних балів
90-100	20	20
82-89	10	зо
75-81	20	50
69-74	10	60
60-68	40	100

Розподіл балів за видами робіт:

Вид роботи	**Бали**	**Вид роботи**	**Бали**
Лабораторна робота 1	3	Самостійна робота 1	2
Лабораторна робота 2	3	Самостійна робота 2	2
Лабораторна робота 3	3	Самостійна робота 3	2
Лабораторна робота 4	3	Самостійна робота 4	2
Лабораторна робота 5	3	Самостійна робота 5	2
Лабораторна робота 6	3	Самостійна робота 6	2
Лабораторна робота 7	3	Самостійна робота 7	2
Лабораторна робота 8	3	Самостійна робота 8	2
Лабораторна робота 9	3	Самостійна робота 9	2
Лабораторна робота 10	3	Самостійна робота 10	2
Лабораторна робота 11	3	Самостійна робота 11	2
Лабораторна робота 12	3	Самостійна робота 12	2
Лабораторна робота 13	3	Самостійна робота 13	2
Лабораторна робота 14	3	Самостійна робота 14	2
Додаткові бали + Захист проєкту	20	Наукова робота	10

Вимоги до критеріїв оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)

40%	Детальний розгляд сутності та вмісту основних джерел. Подання фактів, ідей і результатів досліджень у логічній послідовності. Правильно проаналізовано поточний стан дослідження проблеми та зроблено огляд перспектив подальшого розвитку даного питання.
40%	Обґрунтованість аргументів, підтвердження особистого ставлення, пропозиції стосовно вирішення завдання, встановлення напрямків аналізу.

20%	Оформлення звіту у відповідності вимог
Критерії оцінювання самостійної роботи студента (оцінювання одного завдання у відсотковому еквіваленті)	
100%	В повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі тестові завдання.
80%	Достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та лабораторних завдань, використовуючи при цьому обов'язкову літературу. Але при викладанні деяких питань не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив більшість тестових завдань
60%	В цілому володіє навчальним матеріалом викладає його основний зміст під час усних виступів та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив половину тестових завдань.
40%	Не в повному обсязі володіє навчальним матеріалом. Фрагментарно, поверхово (без аргументації та обґрунтування) викладає його під час усних виступів та письмових відповідей, недостатньо розкриває зміст теоретичних питань та лабораторних завдань, допускаючи при цьому суттєві неточності, правильно вирішив меншість тестових завдань.
20%	Частково володіє навчальним матеріалом не в змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив окремі тестові завдання.
0%	Не володіє навчальним матеріалом та не в змозі його викласти, не розуміє змісту теоретичних питань та практичних завдань. Не вирішив жодного тестового завдання.
ОСНОВНІ ПОЛОЖЕННЯ, ЩО РЕГЛАМЕНТУЮТЬ ОСВІТНІЙ ПРОЦЕС	
діючі положення	https://knute.edu.ua/blog/read/?pid=44402

нормативно-правова база організації освітнього процесу	https://knute.edu.ua/blog/read/?pid=7330&uk
студенту	https://knute.edu.ua/#forstudent
НЕФОРМАЛЬНА ОСВІТА Рекомендовані сертифікаційні програми, курси, посібники користувача	
European Union Agency for Cybersecurity (Агентство Європейського Союзу з питань кібербезпеки)	https://www.enisa.europa.eu
The EU Cyberdiplomacy Toolbox	https://www.cyber-diplomacy-toolbox.com/
MS AZURE	https://learn.microsoft.com/uk-ua/training/azure/
Cloud Native Computing Foundation	https://www.cncf.io/
Isaca	https://www.isaca.org/training-and-events
CSA (Cloud security alliance)	https://cloudsecurityalliance.org/research/artifacts

ПОЛІТИКА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ:

Відвідування лекційних та лабораторних занять: відвідування	Відвідування лекційних та лабораторних занять є обов'язковим. Допускаються пропуски занять з таких поважних причин, як хвороба (викладачу надається копія довідки від медичного закладу), участь в олімпіаді, творчому конкурсі тощо за попередньою домовленістю та згодою викладача за умови дозволу деканату (надаються документи чи інші матеріали, які підтверджують заявлену участь у діяльності студента).
Відпрацювання пропущених занять:	відпрацювання пропущених занять є обов'язковим незалежно від причини пропущеного заняття. Лекційне заняття має бути відпрацьоване до наступної лекції на консультації викладача з використанням ПЗ 365 Office Teams. Відпрацювання лекційного матеріалу передбачає вивчення пропущеного теоретичного матеріалу та складання тесту за цим матеріалом. Лабораторне заняття відпрацьовується під час консультації викладача (розклад консультацій на сайті).
Правила поведінки під час занять	обов'язковим є дотримання техніки безпеки в комп'ютерних лабораторіях. Студенти повинні приймати активну участь в обговоренні навчально матеріалу ознайомившись з ним напередодні (навчальний матеріал надається викладачем). Мобільні пристрої дозволяється використовувати лише під час он-лайн тестування та підготовки практичних завдань в процесі заняття. Задля зручності, дозволяється використання ноутбуків та інших електронних пристроїв під час навчання в

	комп’ютерних аудиторіях (за взаємною згодою всіх учасників освітнього процесу)
Політика академічної доброчесності ДТЕУ	https://knute.edu.ua/blog/read/?pid=38987&uk