ДЕРЖАВНИЙ ТОГРОВЕЛЬНО-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

ЗАТВЕРДЖЕНО
вченою радою
(пост. п. від «4» 03 2024р.)
Ректор
_____Анатолій МАЗАРАКІ

ОСНОВИ КІБЕРДИПЛОМАТІЇ АНГЛІЙСЬКОЮ МОВОЮ/
BASICS OF CYBER DIPLOMACY IN ENGLISH

ПРОГРАМА /
COURSE SUMMARY

Київ 2024

Автори: Олег ГАЙДУК, радник ПРООН з кібердипломатії, ст. викладач,
Андрій ЗАБЛОЦЬКИЙ, експерт з міжнародних відносин, інформаційно комунікаційних технологій та кібердипломатії МЗС України, дипломат

Програму розглянуто і затверджено на засіданні кафедри інженерії програмного забезпечення та кібербезпеки 22 січня 2024 року протокол № 20.

Рецензенти: Геннадій НАДОЛЕНКО, український дипломат, Надзвичайний і Повноважний Посол України, Директор Дипломатичної академії при МЗС України.
Наталія БІЛОУСОВА, доктор наук, професор, завідуюча кафедрою Навчально-наукового інституту Київського національного університету ім. Т. Г. Шевченко.
Валерій ШЕСТАКОВ, полковник, тво директора Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії Служби безпеки України, доктор технічних наук, доцент.
Вадім МАШТІЛІР, полковник, начальник Інституту інформаційно-комунікаційних технологій та кібероборони Національного університету оборони України, заслужений винахідник України, доктор історичних наук, професор.
Олександр КОРНЕЙКО, генерал-майор, завідувач кафедри інформаційних технологій та кібербезпеки Національної академії внутрішніх справ України**,** кандидат технічних наук, професор.
Володимир ТОКАР, д.е.н., професор кафедри інженерії програмного забезпечення та кібербезпеки

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

ПРОГРАМА/
COURSE SUMMARY

ВСТУП

Дисципліна «Основи кібердипломатії англійською мовою» є обов'язковою компонентою навчального підготовки підготовки здобувачів вищої освіти денної та заочної форми навчання другого рівня вищої освіти «магістр» галузі знань 12 «Інформаційні технології» спеціальності 125 «Кібербезпека та захист інформації» ОПП «Безпека систем електронних комунікацій в економіці».

Кібердипломатія є новою галуззю і визначається як вид здійснення дипломатичної діяльності, який являє собою комплекс дій та стратегій, спрямованих на просування та захист національних інтересів і реалізацію зовнішньополітичних цілей України в кіберпросторі, а також підтримання дипломатичних зносин з іноземними державами, їх об'єднаннями та міжнародними організаціями з відповідних питань.

Знаходячись на перетині сфер міжнародного права, дипломатії, інформаційних технологій і кібербезпеки, кібердипломатія стає важливим інструментом просування національних інтересів і зовнішньополітичних цілей країн. Синергія усталеного дипломатичного інструментарію і новітніх можливостей кіберсвіту надає не просто їх арифметичну суму, а принципово нові можливості, що сягають далеко за горизонт звичних уявлень.

Створення нової галузі кібердипломатії для своєї реалізації потребує формування відповідних центрів компетенції в державних установах, представниках крупного бізнесу і у великих громадських організаціях. Така потреба тягне за собою необхідність ґрунтовної підготовки якісних фахівців, які б мали мультідисциплінарну компетенцію одночасно в сферах міжнародних відносин, дипломатії, міжнародного права, юриспруденції, інформаційних технологій, кібербезпеки та володіли б декількома мовами.

Програму підготовлено відповідно до Стандарту вищої освіти України із зазначеної спеціальності та відповідних освітньо-професійних програм підготовки магістрів ДТЕУ.

Програма складається з таких частин:

1. Мета, завдання та предмет дисципліни.
2. Передумови вивчення дисципліни як вибіркової компоненти освітньої програми.
3. Результати вивчення дисципліни.
4. Зміст дисципліни.
5. Список рекомендованих джерел.

1. МЕТА, ЗАВДАННЯ ТА ПРЕДМЕТ ДИСЦИПЛІНИ

Мета вивчення дисципліни «Основи кібердипломатії англійською мовою» полягає у набутті знань, навичок та компетентностей, необхідних для розуміння та ефективного застосування дипломатичних інструментів у в кіберпросторі. Це включає вивчення дипломатичного інструментарію, міжнародних норм, принципів та практик, що регулюють взаємодію держав, недержавних акторів та приватного

сектору у кіберпросторі. Студенти матимуть змогу ознайомитися з концепцією кібердипломатії, її історією, еволюцією та сучасною роллю в міжнародних відносинах. Вони також вивчать основні виклики та проблеми, з якими стикаються уряди та міжнародні організації, коли намагаються забезпечити безпеку та стабільність у кіберпросторі.

Завданням дисципліни «Основи кібердипломатії англійською мовою» є надання студентам знань, навичок та компетентностей, необхідних для розуміння та ефективного застосування дипломатичних інструментів в кіберпросторі. Це включає зокрема відстоювання національних інтересів України в кіберпросторі, вивчення основних викликів та проблем, з якими стикаються уряди та міжнародні організації, аналіз та оцінка політичних, економічних та технологічних чинників, що впливають на міжнародну кібербезпеку, розвиток навичок ефективного спілкування та співпраці з різними зацікавленими сторонами, включаючи уряди, приватні компанії, громадянське суспільство та міжнародні організації, для розробки та впровадження ефективних кіберстратегій та політик

Предмет дисципліни «Основи кібердипломатії англійською мовою» зосереджений на вивченні концепції, практики та викликів кібердипломатії, що є невід'ємною частиною сучасної міжнародної дипломатії, безпеки та політики. Це включає загальне розуміння кібердипломатії, її історію, концепцію і стратегію та сучасну роль у міжнародних відносинах. Вивчення міжнародних норм, принципів та практик, що регулюють взаємодію держав, недержавних акторів та приватного сектору у кіберпросторі. Аналіз політичних, економічних та технологічних чинників, що впливають на дипломатичну діяльність в кіберпросторі. Дослідження основних викликів та проблем, з якими стикаються уряди та міжнародні організації у кіберпросторі. Розвиток навичок ефективного спілкування та співпраці з різними зацікавленими сторонами для розробки та впровадження ефективних кіберстратегій та політик. Розвиток критичного мислення та професійних навичок, необхідних для успішного вирішення складних проблем в цих сферах.

2. ПЕРЕДУМОВИ ВИВЧЕННЯ ДИСЦИПЛІНИ ЯК ВИБІРКОВОЇ КОМПОНЕНТИ ОСВІТНЬОЇ ПРОГРАМИ

знання:

- інформатики (стандартне програмне забезпечення персональних комп’ютерів);
- Project management;
- іноземної мови за професійним спрямуванням;
- мови програмування;
- роботи із базами даних;
- основи міжнародного права
- основи міжнародної діяльності
- основи зовнішньої політики

- англійська мова інформаційних технологій;
- інформаційні технології у професійній діяльності;
- управління проєктами інформатизації/ менеджмент проєтів програмного забезпечення;
- основи кібербезпеки

вміння:

- з офісними додатками Microsoft;
- з хмарними сервісами;
- з пошуковими системами.

3. РЕЗУЛЬТАТИ ВИВЧЕННЯ ДИСЦИПЛІНИ

Дисципліна «Основи кібердипломатії англійською мовою», як обов'язкова компонента освітньої програми «Безпека систем електронних комунікацій в економіці» та вибіркова компонента освітніх програм «Інженерія програмного забезпечення» і «Управління проєктами програмних продуктів», забезпечує оволодіння студентами загальними та фаховими компетентностями і досягнення ними програмних результатів навчання за відповідними освітньо-професійними програмами:

Номер в освітній програмі	Зміст компетентності	Номер теми, що розкриває зміст компетентності
Загальні компетентності за освітньою програмою		
КЗ-1.	Здатність застосовувати знання у практичних ситуаціях.	1-14
КЗ-3.	Здатність до абстрактного мислення, аналізу та синтезу.	1-14
КЗ-5.	Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).	1-14
КЗ-6.	Здатність діяти соціально відповідально та громадсько свідомо.	1-14
КЗ-7.	Здатність до адаптації та дії у новій ситуації.	1-14
КЗ-8.	Здатність до вибору стратегії спілкування, працювати в команді.	1-14
КЗ-9.	Здатність спілкуватися рідною мовою як усно, так і письмово, спілкуватися іноземною мовою (переважно англійською) на рівні, що забезпечує ефективну професійну діяльність.	1-14
Фахові компетентності за освітньою програмою		
КФ-2.	Здатність розробляти, впроваджувати та	1-14

	аналізувати нор¬мативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізу¬вати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.	
КФ4.	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.	1-14
КФ5.	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.	1-14
КФ10.	Здатність провадити науковопедагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.	1-14
КФ12.	Здатність виконувати обов’язки внутрішнього консультанта і радника у своїй експертній області.	1-14
КФ13.	Здатність проводити дослідноекспериментальну роботу щодо процедури сканування вразливостей та їх розпізнавання в системах безпеки.	1-14
Програмні результати навчання за освітньою програмою		
РН1.	Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес\операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	1-14

РН2.	Інтегрувати фундаментальні та спеціальні знання для роз¬в'язування складних задач інформаційної безпеки та/або кібер¬безпеки у широких або мультидисциплінарних контекстах.	1-14
РН3.	Провадити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.	1-14
РН5.	Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізикоматематичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.	1-14
РН7.	Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.	1-14
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.	1-14
РН16.	Приймати обґрунтовані рішення з організаційнотехнічних 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.	1-14
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.	1-14

РН18.	Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напряму інформаційної безпеки та/або кібербезпеки.	1-14
РН25.	Виконувати обов’язки внутрішнього консультанта/ радника в технічній сфері та галузі авторського права щодо електронних носіїв інформації.	1-14

4. ЗМІСТ ДИСЦИПЛІНИ

Тема 1. Кібердипломатія: походження, розвиток, основні принципи, вплив на міжнародні відносини та політику.

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. Вплив кібердипломатії на міжнародну політику. Інструментарій кібердипломатії. Порівняння підходів та стратегій.

Список рекомендованих джерел:
Основний: 1, 2
Додатковий: 1, 2, 3, 4, 5, 6, 23
Інтернет-ресурси: 1, 2, 3, 4, 8, 11, 12

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.

Список рекомендованих джерел:
Основний: 2
Додатковий: 2, 3, 4, 11, 13, 14, 21, 22
Інтернет-ресурси: 1, 2, 3, 5, 6, 7, 9

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.

Список рекомендованих джерел:

Основний: 1, 2 [с. 11-54]
Додатковий: 2, 3, 4, 7, 17, 19, 20
Інтернет-ресурси: 3, 6, 9

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.

Список рекомендованих джерел:
Основний: 1, 3, 4, 5
Додатковий: 1, 2, 3, 7, 8, 9, 10, 16
Інтернет-ресурси: 7, 9, 12

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.

Список рекомендованих джерел:
Основний: 3
Додатковий: 12, 15, 17, 22
Інтернет-ресурси: 7, 9

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.

Список рекомендованих джерел:
Основний: 4, 5
Додатковий: 9, 24
Інтернет-ресурси: 7

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.

Список рекомендованих джерел:
Основний: 4, 5
Додатковий: 9, 10, 24
Інтернет-ресурси: 7, 9

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.

Список рекомендованих джерел:
Основний: 4, 5
Додатковий: 7, 8, 9, 10, 12, 24

Інтернет-ресурси: 7, 8

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.

Список рекомендованих джерел:
Основний: 4, 5
Додатковий: 7, 8, 9, 10, 12, 24
Інтернет-ресурси: 7, 8

Тема 10. Законодавче регулювання ІТ та кібербезпеки, кіберзахисту та кібероборони в Україні, в країнах Європи та Америки, в Азії та країнах Африки.

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: 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.

Список рекомендованих джерел:
Основний: 4, 5
Додатковий: 7, 8, 9, 10, 12, 24
Інтернет-ресурси: 7, 8

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.

Список рекомендованих джерел:

Основний: 1, 2
Додатковий: 1, 2, 3, 4, 5, 6, 23
Інтернет-ресурси: 1, 2, 3, 4, 8, 11, 12

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.

Список рекомендованих джерел:
Основний: 4, 5
Додатковий: 7, 8, 9, 10, 12, 24
Інтернет-ресурси: 7, 8

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. Осінт (Операції інформаційного впливу) в кіберпросторі, їх визначення, цілі та методи. ІПСО та Осінт у контексті міжнародної безпеки та стабільності. Міжнародна співпраця у боротьбі з дезінформацією та Осінт. Роль недержавних суб'єктів у протидії дезінформації та Осінт. Регуляторне середовище для протидії дезінформації та Осінт, національні та міжнародні норми, стандарти та закони. Кібердипломатія та її роль у протидії дезінформації та Осінт.

Список рекомендованих джерел:
Основний: 4, 5
Додатковий: 7, 8, 9, 10, 12, 24
Інтернет-ресурси: 7, 8

Тема 14. Основи штучного інтелекту. Поняття квантових обчислень. Мережі контактних точок.

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 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 Осінт. ШІ та кібердипломатія в контексті міжнародної безпеки та стабільності: виклики, проблеми та потенційні рішення. Освіта та навчання у сфері ШІ.

Список рекомендованих джерел:
Основний: 4, 5
Додатковий: 7, 8, 9, 10, 12, 24
Інтернет-ресурси: 7, 8

5.СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

Основний

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.

Додатковий

1. "Cyber-Diplomacy: Managing Foreign Policy in the Twenty-First Century", Edited By Evan H. Potter. Language: English. Видавництво Mc Gill - Queen's University Press, 2022. -216 с.
2. "Internet Diplomacy. Shaping the Global Politics of Cyberspace": навчальний посібник/Meryem Marzouki, Andrea Calderaro. Language: English. Видавництво Rowman & Littlefield Publishers, 2023. -280 с.
3. "Science Diplomacy, Cyberdiplomacy and Techplomacy in EU-LAC Relations" Mario Torres Jarrín, Shaun Riordan. Language: English. Видавництво Springer Cham, 2023. -180 с.
4. Дипломатична та консульська служба. Навч. посіб./ Я.Б. Турчин, О. Н. Горбач, Л. О. Дорош, О. Я. Івасечко, У.В. Ільницька. Львів: Видавництво Львівської політехніки, 2014. 224 с.

5. Головченко В. Дипломатична історія України: підручник / В. Головченко, В. Матвієнко. Київ: Ніка-Центр, 2018. 420 с.
6. Панов А.В. Дипломатична і консульська служба: підручник. Ужгород: Аутдор-Шарк, 2015. 270 с.
7. *Гамова І. В. Інформаційні війни: підручник / І. В. Гамова. – Київ: Держ. торг.-екон. ун-т, 2022. – 184 с.*
8. Калініченко Б.М. Інформаційна війна: чинники ескалації та засоби протидії: підручник // Б.М. Калініченко. – Черкаси: Видавець Чабаненко Ю., 2020. – 350 с.
9. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок, Р. В. Киричок, П. М. Складанний – К., 2018. – 320 с.
10. Безпека інформаційних систем: навч. посіб. / В. І. Пашорін, Ю. В. Костюк. – Київ: Держ. торг.-екон. ун-т, 2022. – 376 с.
11. Атаманенко А. Роль закордонних українців в публічній та культурній дипломатії: історичний і сучасний аспекти. Наукові записки Нац. ун-ту «Острозька академія». 2019. № 29. Сер. «Історичні науки». С. 54-65.
12. Адміністративно-правове регулювання охорони Національною гвардією України дипломатичних представництв іноземних держав / О.С. Конопляник, С.К. Гречанюк, В.О. Галай [Монографія]. Київ: ГО «Київський правозахисний альянс», 2016. 182 с.
13. *Бохан А.В. Екологічна дипломатія в інтерактивній модальності глобалізації: монографія. Київ: Київ. нац. торг.-екон. ун-т, 2018. 456 с.*
14. *Бохан А.В. Екологічні застороги в дипломатії миру і торгівлі. Зовнішня торгівля: економіка, фінанси, право. 2017. №4 (93). С. 71-83.*
15. Войціховський А.В. Міжнародне право: підручник: Харків: Харк. нац. ун-т внутрішніх справ, 2020. 543 с.
16. Григор О.О. Сучасні виміри дипломатії в умовах конфліктних і кризових ситуацій. Політикус. 2019. Вип. 2. С. 79-84.
17. Григор О.О. Ефективна дипломатія як чинник дося досягнення політичного консенсусу. Гілея: науковий вісник. 2015. Вип. 95. С. 356-360.
18. *Дипломатична та консульська служба. Опорний конспект лекцій. /О.В. Кам'янецька. Київ: Київ. нац. торг.-екон. ун-т, 2018. 79 с.*
19. Дипломатическая служба зарубежных стран: Учебник / Под ред. А.В. Торкунова, А.Н. Панова. М.: Аспект Пресс, 2019. 400 с.
20. Дипломатична та консульська служба у вимірі особистості. Київ: Генеральна дирекція з обслуговування іноземних представництв. 2019. Ч. 2. 296 с.
21. Дипломатичний протокол та етикет: підручник / О.П. Сагайдак. 2-ге вид., оновл. і доповн. Київ: Знання, 2017. 326 с.
22. Дипломатія / Генрі Кіссинджер; пер. з англ. М. Гоцацюка, В. Горбатька. Київ: Вид. група. КМ-БУКС, 2020. 864 с.
23. *Євроінтеграційні пріоритети національного бізнесу: монографія / за заг. ред. А.А. Мазаракі. Київ.: Київ. нац. торг-екон. ун-т, 2018. 672 с.*

24. Указ Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року "Про Стратегію кібербезпеки України" (дата звернення: 30.06.2022).
25. Закон України «Про основні засади забезпечення кібербезпеки України» // Відомості Верховної Ради України, 2017. – № 45. – Ст.403.
26. Закон України «Про оборону України» // Відомості Верховної Ради України. – 2017. – № 45. – Ст.403.

Інтернет-ресурси

1. Віденська конвенція про дипломатичні зносини (18.04.1961). URL: https://zakon.rada.gov.ua/laws/show/995_048#Text
2. Віденська конвенція про консульські зносини (24.04.1963). https://zakon.rada.gov.ua/laws/show/995_047#Text
3. Закон України «Про дипломатичну службу» № 2449-VIII від 07.06.2018. URL: https://zakon.rada.gov.ua/laws/show/2449-19#Text
4. Закон України «Про засади внутрішньої та зовнішньої політики» №2411- VI від 01.07.2010. URL: https://zakon.rada.gov.ua/laws/show/2411-17#Text
5. Указ Президента України «Про Програму розміщення дипломатичних представництв, консульських установ іноземних держав і представництв міжнародних організацій в Україні» URL: https://zakon.rada.gov.ua/laws/show/517/94#Text
6. Закордонні дипломатичні установи URL: https://taxlink.ua/ua/analytics/bjudzetne-zakonodavstvo/zakordonni-diplomatichni-ustanovi-ukraini/
7. European union agency for cybersecurity. URL: https://www.enisa.europa.eu
8. https://cyberdiplomacy.net/
9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
10. https://afsa.org/diplomacy-cyberspace
11. https://cyberdiplomacy.disarmamenteducation.org/home/
12. https://www.state.gov/about-us-bureau-of-cyberspace-and-digital-policy/