МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ

ЗАТВЕРДЖЕНО
на засіданні кафедри
міжнародних відносин і політичної
філософії
Протокол № 17 від 28.08.2025 р.

ПОГОДЖЕНО
Проректор з навчально-методичної
роботи
_____ Каріна НЕМАШКАЛО

КІБЕРДИПЛОМАТІЯ
робоча програма навчальної дисципліни (РПНД)

Галузь знань	**С «Соціальні науки, журналістика, інформація та міжнародні відносини»**
Спеціальність	**С3 «Міжнародні відносини»**
Освітній рівень	**Перший (бакалаврський)**
Освітня програма	**Міжнародні відносини**

Статус дисципліни	**вибіркова**
Мова викладання, навчання та оцінювання	**українська**

Розробник:
викл. _____ Данило НЕПОЧАТОВ

Завідувач кафедри
міжнародних відносин і
політичної філософії _____ Олег КУЗЬ

Гарант програми _____ Ірина ЖЕРЕБЯТНІКОВА

Харків
2025

ВСТУП

Навчальна дисципліна «Кібердипломатія» є вибірковою навчальною дисципліною професійного циклу підготовки бакалаврів за спеціальністю С3 «Міжнародні відносини». Актуальність дисципліни зумовлена трансформацією кіберпростору на один із ключових вимірів міжнародної безпеки, у межах якого відбувається конкуренція держав, формуються нові конфліктні динаміки та виникає потреба в дипломатичних механізмах регулювання цифрових загроз.

У сучасних міжнародних відносинах кібератаки, операції впливу, проблеми атрибуції та асиметрії технологічних можливостей дедалі частіше виступають факторами стратегічної нестабільності. За цих умов кібердипломатія формується як інструмент зовнішньої політики, спрямований на управління конфліктами низької інтенсивності у кіберпросторі, запобігання ескалації, вироблення міжнародних норм поведінки та забезпечення передбачуваності у сфері міжнародної кібербезпеки.

Навчальна дисципліна розглядає кібердипломатію не лише як сукупність дипломатичних практик, але як емпірично спостережуваний і аналітично вимірюваний процес міжнародної взаємодії. У межах курсу здобувачі опановують підходи до аналізу кіберінцидентів, дипломатичних заяв, переговорних форматів і стратегічних документів, що дозволяє інтерпретувати події у кіберпросторі як елементи ширшої системи міжнародної безпеки.

Курс ґрунтується на поєднанні якісного політико-безпекового аналізу з елементами data-driven та computational підходів, що дає змогу виявляти структурні тенденції, акторні конфігурації та патерни поведінки держав і міжнародних організацій у глобальному кіберпросторі. Такий підхід дозволяє відійти від описового рівня й сформувати у здобувачів навички системного аналітичного мислення.

Навчальний матеріал базується на аналізі репрезентативних кейсів кібердипломатичної практики, які ілюструють різні моделі забезпечення кібербезпеки, підходи до міжнародного нормотворення, а також особливості взаємодії між державними та недержавними акторами у цифровому середовищі. Особлива увага приділяється кейсам, пов’язаним із геополітичною конкуренцією, кризами та збройними конфліктами.

Об’єктом навчальної дисципліни є кібердипломатія як складова міжнародної кібербезпеки та форма взаємодії суб’єктів міжнародних відносин у кіберпросторі.

Предметом навчальної дисципліни є політичні, правові, інституційні та технологічні чинники формування міжнародних норм, дипломатичних стратегій, механізмів стримування та співпраці у сфері кібербезпеки.

Метою навчальної дисципліни є формування у здобувачів здатності концептуально осмислювати кібердипломатію як інструмент міжнародної кібербезпеки, а також аналізувати процеси формування норм, стратегій і практик міжнародної взаємодії у кіберпросторі з використанням порівняльного, кейсового та data-driven підходів.

Завдання навчальної дисципліни:

- сформувати теоретичне розуміння кіберпростору як специфічного домену міжнародної безпеки, у якому поєднуються політичні, військові, правові та технологічні виміри;
- проаналізувати кібердипломатію як інструмент управління конфліктами, деескалації та формування передбачуваних моделей поведінки держав у середовищі обмеженої прозорості та складної атрибуції;
- ознайомити з ключовими підходами до міжнародного нормотворення у кіберпросторі в межах багатосторонніх і регіональних форматів;
- сформувати здатність критично аналізувати національні та міжнародні кіберстратегії у контексті зовнішньої політики та міжнародної безпеки;
- навчити інтерпретувати кіберінциденти як політичні сигнали та інструменти стратегічної комунікації у міжнародних відносинах;
- опанувати базові навички підготовки аналітичних матеріалів, policy briefs та рекомендацій у сфері кібердипломатії;
- розвинути здатність поєднувати якісний кейс-аналіз з елементами data-driven та OSINT-аналізу для виявлення акторів і патернів міжнародної взаємодії у кіберпросторі;
- сформувати розуміння обмежень і ризиків кібердипломатії, зокрема проблем ескалації, асиметрії можливостей та інструменталізації міжнародного права.

Результати навчання та компетентності, які формує навчальна дисципліна, визначено в табл. 1.

Таблиця 1

Результати навчання та компетентності, які формує навчальна дисципліна

Результати навчання	Компетентності, якими повинен оволодіти здобувач вищої освіти
РН2.	ЗК5, СК1, СК3, СК11.
РН3.	ЗК5, СК1, СК13.
РН7.	ЗК6, СК2, СК4.
РН8.	ЗК12, СК3, СК4, СК12.
РН9.	ЗК5, ЗК12, СК11, СК13.
РН10.	ЗК11, СК12.
РН11.	СК4, СК10, СК13.
РН14.	СК3, СК4, СК5, СК12.

де, РН02. Знати та розуміти природу та динаміку міжнародної безпеки, розуміти особливості її забезпечення на глобальному, регіональному та національному рівні, знати природу та підходи до вирішення міжнародних та інтернаціоналізованих конфліктів.

РН05. Знати природу та механізми міжнародних комунікацій.

РН07. Здійснювати опис та аналіз міжнародної ситуації, збирати з різних джерел необхідну для цього інформацію про міжнародні та зовнішньополітичні події та процеси.

РН08. Збирати, обробляти та аналізувати великі обсяги інформації про стан міжнародних відносин, зовнішньої політики України та інших держав, регіональних систем, міжнародних комунікацій.

РН09. Досліджувати проблеми міжнародних відносин, регіонального розвитку, зовнішньої політики, міжнародних комунікацій, із використанням сучасних політичних, економічних і правових теорій та концепцій, наукових методів та міждисциплінарних підходів, презентувати результати досліджень, надавати відповідні рекомендації.

РН10. Вільно спілкуватися державною та іноземними мовами на професійному рівні, необхідному для ведення професійної дискусії, підготовки аналітичних та дослідницьких документів.

РН11. Здійснювати прикладний аналіз міжнародних відносин, зовнішньої політики України та інших держав, міжнародних процесів та міжнародної ситуації відповідно до поставлених цілей, готувати інформаційні та аналітичні матеріали.

РН14. Використовувати сучасні цифрові технології, спеціалізовані програмне забезпечення, бази даних та інформаційні системи для розв’язання

складних спеціалізованих задач у сфері міжнародних відносин, суспільних комунікацій та/або регіональних студій.

ЗК5. Здатність працювати в міжнародному контексті.

ЗК6. Здатність генерувати нові ідеї (креативність).

ЗК11. Здатність спілкуватися іноземною мовою.

ЗК12 – Здатність до пошуку, оброблення та аналізу інформації з різних джерел.

СК1. Здатність виокремлювати ознаки та тенденції розвитку, розуміти природу, динаміку, принципи організації міжнародних відносин, суспільних комунікацій та/або регіональних студій.

СК2 – Здатність аналізувати міжнародні процеси у різних контекстах (політичному, культурному, інформаційному тощо).

СК3 – Здатність оцінювати стан і напрями досліджень міжнародних відносин та світової політики.

СК4 – Здатність розв’язувати складні спеціалізовані задачі і практичні проблеми у сфері міжнародних відносин та суспільних комунікацій.

СК5 – Здатність аналізувати вплив світової економіки, міжнародного права та внутрішньої політики на міжнародні відносини.

СК10 – Здатність аналізувати структуру та динаміку міжнародних суспільних комунікацій.

СК11 – Здатність аналізувати природу та еволюцію міжнародних організацій.

СК12 – Здатність до здійснення комунікації та інформаційно-аналітичної діяльності у сфері міжнародних відносин.

СК13 – Здатність аналізувати діяльність міжнародних недержавних акторів та транснаціональні відносини.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Вступ до кібердипломатії: кіберпростір як вимір міжнародної безпеки

Тема окреслює предмет і логіку курсу, пояснюючи, чому кіберпростір став самостійним виміром міжнародної безпеки поряд із сушею, морем, повітрям і космосом. Аналіз трансформації цифрових загроз із технічної проблеми у політико-безпековий виклик. Кібердипломатія розглядається як інструмент управління ризиками, конфліктами та міжнародною взаємодією у цифровому середовищі.

Ключові питання:

- Чому кіберпростір є доменом міжнародної безпеки?
- У чому полягає сутність кібердипломатії як дипломатичної практики?
- Які виклики кіберпростір створює для традиційної дипломатії?

Тема 2. Актори кібердипломатії та структура глобального кіберпростору

Тема присвячена аналізу ключових акторів кібердипломатії та їхніх ролей у формуванні міжнародного порядку в кіберпросторі. Розглядається взаємодія держав, міжнародних організацій, приватних технологічних компаній і експертних спільнот. Приділено увагу асиметрії можливостей і впливу між різними групами акторів.

Ключові питання:

- Хто є головними акторами кібердипломатії?
- Чому недержавні актори відіграють критичну роль у кібербезпеці?
- Як асиметрія ресурсів впливає на міжнародну кіберстабільність?

Тема 3. Глобальний ландшафт кіберзагроз і логіка конфлікту в кіберпросторі

У темі розкрито основні типи кіберзагроз та їхню роль у сучасних міжнародних конфліктах. Кіберінциденти розглядаються як форма політичного сигналу, примусу або стримування. Окрема увага приділяється проблемі атрибуції та обмеженій передбачуваності дій у кіберпросторі.

Ключові питання:

- Які типи кіберзагроз мають стратегічне значення?
- Чим кіберконфлікти відрізняються від традиційних воєнних конфліктів?
- Як проблема атрибуції впливає на ескалацію?

Тема 4. Кібердипломатія провідних держав: стратегічні моделі США та Китаю

Тема присвячена порівняльному аналізу кібердипломатії США та Китаю як двох конкуруючих моделей глобального впливу. Розглядаються відмінності у

підходах до нормотворення, стримування та ролі держави у кіберпросторі. Аналізується, як кібердипломатія інтегрується у ширшу геополітичну конкуренцію.

Ключові питання:

- У чому полягають ключові відмінності кіберстратегій США та Китаю?
- Як кібердипломатія відображає глобальну конкуренцію великих держав?
- Які наслідки цієї конкуренції для міжнародної кібербезпеки?

Тема 5. Кібердипломатія України: безпекова оптика та міжнародна взаємодія

Тема розглядає специфіку кібердипломатії України в умовах збройного конфлікту та гібридної війни. Аналізується роль міжнародної підтримки, партнерств і правових механізмів у забезпеченні кіберстійкості. Особлива увага приділяється практичному досвіду України як джерелу міжнародних уроків.

Ключові питання:

- Яке місце України у глобальній системі кібербезпеки?
- Як війна трансформує інструменти кібердипломатії?
- Які уроки українського досвіду є релевантними для інших держав?

Тема 6. Міжнародне право, норми та цифровий суверенітет у кіберпросторі

Тема аналізує міжнародно-правові основи регулювання кіберпростору та проблеми формування загальноприйнятих світових норм. Розглядаються концепції цифрового суверенітету, державної відповідальності та правових меж кіберактивності. Окремо аналізується напруга між безпекою, свободами та міжнародним правом.

Ключові питання:

- Чи можливе ефективне міжнародне право у кіберпросторі?
- Як держави інтерпретують цифровий суверенітет?
- Де проходить межа між безпекою та правами людини у кіберпросторі?

Тема 7. Кіберзброя, стримування та ескалація в міжнародних конфліктах

Тема присвячена аналізу кіберзброї як інструменту міжнародного протистояння. Розглядаються концепції кіберстримування, ризики ескалації та проблеми контролю над кіберарсеналами. Акцент зроблено на стратегічній невизначеності та непрозорості кібероперацій.

Ключові питання:

- Чи можна вважати кібероперації формою застосування сили?
- Як працює стримування у кіберпросторі?
- Які ризики ескалації пов’язані з кіберзброєю?

Тема 8. Технологічний вимір кібердипломатії: ШІ, напівпровідники, критична інфраструктура

Тема аналізує новітні технології як ключовий чинник міжнародної кібербезпеки та дипломатії. Розглядається роль штучного інтелекту, напівпровідників і захисту критичної інфраструктури у формуванні безпекових залежностей. Технології подаються як об'єкт стратегічного контролю та дипломатичних домовленостей.

Ключові питання:

- Чому технології стали предметом міжнародної дипломатії?
- Як технологічні ланцюги впливають на безпеку держав?
- Які ризики та можливості несе ШІ для кібердипломатії?

Тема 9. Кібердипломатія та економічна безпека

Тема присвячена взаємозв'язку кібербезпеки, глобальної економіки та технологічних ринків. Аналізуються санкції, експортний контроль і технологічні обмеження як інструменти кібердипломатії. Розглядається економічна вразливість як фактор міжнародної кіберстабільності.

Ключові питання:

- Як кібербезпека впливає на економічну безпеку держав?
- Чи можна говорити про економічну кібердипломатію?
- Яку роль відіграють технологічні санкції у міжнародних відносинах?

Тема 10. Синтез і майбутні тенденції кібердипломатії

Підсумкова тема інтегрує теоретичні та прикладні підходи курсу та формує цілісне бачення кібердипломатії. Аналізуються майбутні тенденції міжнародної кібербезпеки та вимоги до аналітичної і дипломатичної роботи. Тема орієнтована на підготовку до практичного застосування знань.

Ключові питання:

- Які тенденції визначатимуть майбутнє кібердипломатії?
- Які компетентності потрібні фахівцю з міжнародної кібербезпеки?
- Як перетворювати аналіз кіберподій на політичні рішення?

Перелік практичних (семінарських) занять / завдань за навчальною дисципліною наведено в табл. 2

Таблиця 2

Перелік практичних (семінарських) занять

Назви тем	Зміст
Завдання 1 Тема 1. Вступ до кібердипломатії: кіберпростір як вимір міжнародної безпеки	*Індивідуальне завдання:* упродовж 7 днів зібрати базовий датасет для 10–15 країн у форматі країна–рік та побудувати 2 графіки розподілу показників кібербезпеки. *Дані*: GCI, NCSI, Polity2 або Freedom House. *Інструменти:* R, readr/readxl, dplyr, ggplot2. *Групове завдання (етап 1):* формування єдиного формату панельного датасету для семестрового проєкту.
Завдання 2 Тема 2. Актори кібердипломатії та структура глобального кіберпростору	*Індивідуальне завдання:* на основі підготовленого датасету здійснити порівняльний аналіз двох груп держав (наприклад, демократичних і авторитарних) за показниками кібербезпеки. Використати описову статистику та візуалізації для виявлення відмінностей між групами. Інтерпретувати результати з урахуванням ролі держави як актора кібердипломатії. Сформулювати попередні аналітичні висновки. *Дані:* GCI або NCSI, Polity2 або Freedom House. *Інструменти:* R, dplyr, ggplot2. *Групове завдання (етап 2)*: Узгодження переліку країн і часових меж групового дослідження.
Завдання 3 Тема 3. Глобальний ландшафт кіберзагроз і логіка конфлікту в кіберпросторі	*Індивідуальне завдання:* побудувати часові тренди показників кібербезпеки та проаналізувати їхню динаміку. Коротко оцінити стабільність або мінливість кібербезпекового середовища. *Дані:* GCI або NCSI за кілька років, Digital Development Index. *Інструменти:* R, lubridate, ggplot2 Групове завдання (етап 3): сформулювати 2–3 аналітичні гіпотези, які будуть перевірятися в межах групового проєкту. Узгодити, які показники використовуються для їх перевірки. Зафіксувати гіпотези у спільному документі.
Завдання 4	*Індивідуальне завдання:* розрахувати кореляції між

Тема 3. Глобальний ландшафт кіберзагроз і логіка конфлікту в кіберпросторі	кількома індексами кібербезпеки та показниками політичного режиму. Побудувати кореляційну матрицю та візуалізувати її у вигляді теплової карти. Проаналізувати, які показники є найбільш узгодженими між собою, а які демонструють розбіжності. Зробити висновок щодо того, що саме вимірюють різні індекси. *Дані:* GCI, NCSI, EGDI, Digital Development Index, Cyber Risk Index, Internet penetration, Polity2, Freedom House. *Інструменти:* R, cor, ggcorrplot. *Групове завдання (етап 4):* відібрати ключові змінні для подальшого групового аналізу. Обґрунтувати вибір кожної змінної з аналітичної точки зору. Зафіксувати фінальний набір показників..
Завдання 5 Тема 4. Кібердипломатія провідних держав: стратегічні моделі США та Китаю	*Індивідуальне завдання:* застосувати метод головних компонент або кластерний аналіз до набору показників кібербезпеки. Визначити основні аналітичні виміри та інтерпретувати їхній зміст. Візуалізувати результати та пояснити, як вони спрощують розуміння складного набору даних. Коротко оцінити аналітичну цінність отриманих компонентів або кластерів. *Дані:* 6–8 кількісних індексів кібербезпеки. *Інструменти:* R, FactoMineR, factoextra *Групове завдання (етап 5):* узгодити перелік аналітичних вимірів, які будуть використані в груповому проєкті. Співвіднести їх із попередньо сформульованими гіпотезами. Зафіксувати структуру аналітичної моделі групового дослідження.
Завдання 6 Тема 4. Кібердипломатія провідних держав: стратегічні моделі США та Китаю	*Індивідуальне завдання:* на основі підготовленого датасету дослідити зв’язок між типом політичного режиму та рівнем кібербезпеки, перевіривши, чи є цей зв’язок нелінійним. Побудувати графік з локальною регресією (LOESS) та порівняти його з лінійною моделлю. За бажанням застосувати GAM для більш формалізованої перевірки нелінійності. Коротко інтерпретувати, у яких діапазонах показників режиму зв’язок змінюється. *Дані:* Polity2 або Freedom House, GCI або EGDI

	Інструменти: R, ggplot2 (LOESS), mgcv *Групове завдання (етап 6):* Обговорити в групах виявлені нелінійні патерни та зафіксувати, чи вони повторюються для різних країн або регіонів. Визначити, які з цих патернів доцільно включити до групового аналітичного звіту. Сформулювати попередні пояснювальні гіпотези.
Завдання 7 Тема 5. Кібердипломатія України: безпекова оптика та міжнародна взаємодія	*Індивідуальне завдання:* на основі побудованої моделі визначити країни, показники кібербезпеки яких суттєво відхиляються від прогнозованих значень. Проаналізувати залишки моделі та ідентифікувати позитивні й негативні аномалії. Для 1–2 країн підготувати коротке пояснення можливих причин відхилення з урахуванням політичного або безпекового контексту. *Дані:* показники кібербезпеки, залишки регресійних моделей *Інструменти:* R, broom, dplyr, ggplot2 *Групове завдання (етап 7):* колективно відібрати 2–3 країни, які становлять найбільший аналітичний інтерес як "відхилення від очікуваного". Узгодити, які з них будуть розглянуті як кейси у фінальному груповому проєкті. Розподілити країни між учасниками групи.
Завдання 8 Тема 6. Міжнародне право, норми та цифровий суверенітет у кіберпросторі	*Індивідуальне завдання:* завантажити тексти стратегічних документів у сфері кібербезпеки та підготувати їх до аналізу як корпус даних. Здійснити частотний аналіз ключових термінів і базову очистку тексту. Визначити, які поняття та категорії найчастіше використовуються у кібердипломатичному дискурсі обраного актора. *Дані:* національні кіберстратегії, документи UN / EU / NATO. *Інструменти:* R, quanteda, tidytext. *Групове завдання (етап 8):* сформувати спільний корпус документів для групового аналізу, узгодивши критерії відбору текстів. Розподілити документи між членами групи для подальшої обробки. Зафіксувати структуру корпусу та метадані.
Завдання 9	*Індивідуальне завдання:* порівняти кібернаративи двох

Тема 7. Кіберзброя, стримування та ескалація в міжнародних конфліктах	держав або міжнародних організацій шляхом аналізу ключових слів і термінів. Застосувати показники tf-idf для виявлення специфічних тем і акцентів. Зробити висновок про відмінності у підходах до кібердипломатії та міжнародної кібербезпеки. *Дані:* корпуси стратегічних і програмних документів *Інструменти:* R, quanteda, tf-idf *Групове завдання (етап 9):* узгодити спільну рамку інтерпретації текстових результатів для групового проєкту. Визначити, які наративні відмінності є найбільш значущими для аналітичних висновків. Сформулювати попередні узагальнення.
Завдання 10 Тема 8. Технологічний вимір кібердипломатії: ШІ, напівпровідники, критична інфраструктура	*Індивідуальне завдання*: на основі подієвого датасету побудувати часовий аналіз кіберінцидентів та пов'язаних дипломатичних реакцій. Візуалізувати зміну інтенсивності подій у часі та визначити ключові піки. Коротко проаналізувати, як кіберінциденти співвідносяться з дипломатичними діями. *Дані:* подієвий датасет (дата, країна, тип події) *Інструменти:* R, lubridate, ggplot2 *Групове завдання (етап 10):* інтегрувати подієві дані з раніше зібраними структурними показниками. Узгодити, як подієвий аналіз доповнює загальну логіку групового дослідження. Визначити, які події будуть включені у фінальний аналіз.
Завдання 11 Тема 8. Технологічний вимір кібердипломатії: ШІ, напівпровідники, критична інфраструктура	*Індивідуальне завдання:* на основі проведеного аналізу підготувати короткий policy brief із формулюванням основних висновків і рекомендацій. Особливу увагу приділити логіці переходу від даних до практичних політичних рішень. Чітко зазначити обмеження аналізу та можливі альтернативні інтерпретації. *Дані:* результати індивідуальних аналітичних завдань *Інструменти:* RMarkdown або Quarto *Групове завдання (етап 11):* сформувати спільні висновки та рекомендації групового проєкту. Узгодити структуру фінального аналітичного звіту. Розподілити

	відповідальність за розділи документа.
Завдання 12 Тема 9. Кібердипломатія та економічна безпека	*Індивідуальне завдання:* підготувати коротку методологічну рефлексію щодо використаних даних і методів аналізу. Оцінити сильні та слабкі сторони обраного підходу. Запропонувати можливі напрями вдосконалення дослідження. *Дані:* фінальний груповий датасет, результати аналізу *Інструменти:* R, презентаційні засоби Групове завдання (етап 12): фіналізація візуальних матеріалів презентації.
Завдання 13 Тема 9. Кібердипломатія та економічна безпека	*Індивідуальне завдання:* на основі всіх виконаних протягом семестру аналітичних завдань підготувати узагальнювальний аналітичний огляд. Систематизувати застосовані дані, методи та отримані результати, виокремивши ключові аналітичні висновки щодо міжнародної кібербезпеки та кібердипломатії. Критично оцінити обмеження використаних індексів, моделей і джерел даних, а також їхню придатність для практичної політики. Сформулювати власне бачення того, як computational-підходи можуть бути використані у подальших дослідженнях або професійній діяльності у сфері міжнародних відносин. *Дані:* результати всіх індивідуальних і групових завдань курсу *Інструменти:* RMarkdown або Quarto
Завдання 14 Тема 10. Синтез і майбутні тенденції кібердипломатії	Презентація групового проєкту з кібердипломатії. Захистити аналітичні висновки та відповісти на запитання. Узагальнити досвід командної роботи протягом семестру.

Перелік самостійної роботи за навчальною дисципліною наведено в табл. 3.

Таблиця 3

Перелік самостійної роботи

Завдання	Зміст

Завдання 1	Самостійне ознайомлення з базовими поняттями міжнародної кібербезпеки та кібердипломатії. Збір базових кількісних даних для 10–15 держав у форматі країна–рік (показники кібербезпеки, тип політичного режиму, регіон). Первинна структуризація даних та побудова графіків розподілу й регіонального порівняння з використанням мови програмування R.
Завдання 2	Самостійний порівняльний аналіз двох груп держав (наприклад, демократій і авторитарних режимів) за показниками кібербезпеки. Застосування описової статистики та візуалізацій для виявлення відмінностей між групами. Формулювання попередніх аналітичних висновків щодо ролі держав у кібердипломатії.
Завдання 3	Самостійна побудова часових рядів показників кібербезпеки для обраних країн за кілька років. Аналіз динаміки, виявлення трендів і можливих переломних моментів у розвитку кібербезпекового середовища. Порівняння динаміки між країнами або регіонами з використанням мови програмування R.
Завдання 4	Самостійний розрахунок кореляцій між кількома індексами кібербезпеки та показниками політичного режиму. Побудова кореляційної матриці та її візуалізація у вигляді теплової карти. Аналітична оцінка узгодженості індексів і їхньої концептуальної відмінності.
Завдання 5	Самостійне застосування методів зменшення розмірності або кластерного аналізу до набору показників кібербезпеки. Інтерпретація отриманих компонентів або кластерів як аналітичних вимірів кібербезпеки. Оцінка їхньої придатності для подальшого порівняльного аналізу.
Завдання 6	Самостійне дослідження нелінійних зв’язків між типом політичного режиму та рівнем кібербезпеки. Побудова локальних і узагальнених моделей (LOESS або GAM) та порівняння їх із лінійними підходами. Аналітична інтерпретація отриманих залежностей з використанням мови програмування R.
Завдання 7	Самостійний аналіз аномалій у показниках кібербезпеки шляхом дослідження залишків регресійних моделей. Виявлення країн, що демонструють істотні відхилення від очікуваних значень.

	Підготовка короткого пояснення можливих причин таких відхилень.
Завдання 8	Самостійне формування корпусу офіційних документів у сфері кібербезпеки та кібердипломатії (національні стратегії, міжнародні декларації). Проведення частотного аналізу ключових термінів і базової обробки текстових даних з використанням мови програмування R.
Завдання 9	Самостійний порівняльний аналіз кібернаративів двох держав або міжнародних організацій. Застосування методів аналізу ключових слів і показників tf-idf для виявлення відмінностей у підходах до кібердипломатії. Формулювання змістовних висновків на основі текстових даних.
Завдання 10	Самостійний подієвий аналіз кіберінцидентів і пов'язаних із ними дипломатичних реакцій. Побудова часових візуалізацій та аналіз інтенсивності подій. Оцінка взаємозв'язку між кіберінцидентами та міжнародною дипломатичною активністю.
Завдання 11	Самостійна підготовка індивідуального аналітичного policy brief на основі виконаних computational-завдань. Формулювання висновків і рекомендацій для сфери міжнародної кібербезпеки з обов'язковим зазначенням методологічних обмежень аналізу.
Завдання 12	Самостійна підготовка короткої методологічної рефлексії щодо використаних упродовж семестру даних і методів аналізу. Оцінка сильних і слабких сторін обраного computational-підходу, а також обмежень фінального групового датасету й аналітичних моделей. Формулювання можливих напрямів удосконалення дослідження та альтернативних методологічних рішень.
Завдання 13	Самостійна підготовка узагальнювального аналітичного огляду на основі всіх виконаних протягом семестру індивідуальних і групових завдань. Систематизація застосованих даних, методів і отриманих результатів з виокремленням ключових аналітичних висновків щодо міжнародної кібербезпеки та кібердипломатії. Критична оцінка придатності використаних індексів, моделей і джерел даних для формування практичних політичних рішень, а також формулювання власного бачення подальшого застосування computational-підходів у дослідженнях і

	професійній діяльності у сфері міжнародних відносин.
Завдання 14	Семестровий груповий проєкт «Cyber Diplomacy Intelligence Project» виконується здобувачами у групах по 2–3 особи впродовж семестру. Проєкт передбачає поетапне формування та аналіз спільного датасету міжнародної кібербезпеки й кібердипломатії. У кінці семестру відбувається захист групових проєктів у форматі review. Проєкт кожної групи має містити: - структурований панельний датасет (країна–рік) із показниками кібербезпеки, політичного режиму та додатковими змінними; - аналітичні візуалізації динаміки та порівняльних показників; - результати кореляційного, кластерного та нелінійного аналізу; - аналіз аномалій і кейси країн-відхилень; - корпус офіційних документів і результати text-as-data аналізу; - подієвий аналіз кіберінцидентів і дипломатичних реакцій; - відтворюваний аналітичний звіт (R-скрипти або Quarto/R Markdown); - фінальний аналітичний документ — Cyber Diplomacy Intelligence Brief з розділом «Методи та обмеження»; - презентацію результатів групового проєкту.

МЕТОДИ НАВЧАННЯ

Під час викладання навчальної дисципліни «Кібердипломатія» використовуються традиційні та інноваційні методи організації навчального процесу, спрямовані на формування у здобувачів системного розуміння кібердипломатії як інструменту міжнародної кібербезпеки, а також навичок аналітичної роботи з кількісними, подієвими та текстовими даними у сфері міжнародних відносин. Особлива увага приділяється застосуванню computational-підходів, критичній інтерпретації індексів і моделей кібербезпеки та поєднанню емпіричного аналізу з політико-дипломатичним контекстом.

Навчальний процес поєднує лекційні, практичні, семінарські та дослідницько-проєктні формати, з акцентом на самостійну та групову аналітичну

діяльність, виконання computational-завдань і підготовку семестрового групового аналітичного проєкту з кібердипломатії.

Словесні методи:

- лекція з елементами аналітичного огляду глобального середовища міжнародної кібербезпеки та ролі кібердипломатії у ньому (Теми 1, 2, 10);
- проблемна лекція, спрямована на постановку дослідницьких питань, формування аналітичних гіпотез і критичне осмислення підходів до вимірювання кібербезпеки (Теми 1, 3, 6);
- міні-лекція з поясненням теоретичних і концептуальних підходів до аналізу кібердипломатії, кіберсуверенітету, міжнародних норм поведінки у кіберпросторі та моделей кіберврядування (Теми 3, 5, 7, 9).

Наочні методи:

- демонстрація та аналіз міжнародних індексів кібербезпеки, карт кіберзагроз і візуальних моделей цифрової нерівності між державами (Теми 1–4);
- використання статистичних візуалізацій, часових рядів, кореляційних матриць, кластерних і подієвих графіків, створених у середовищі R (Теми 2–10);
- презентація результатів індивідуального та групового computational-аналізу, включно з візуальними матеріалами семестрового проєкту (Теми 12–14).

Практичні методи:

- виконання індивідуальних computational-завдань зі збору, структурування та аналізу даних міжнародної кібербезпеки з використанням мови програмування R (Теми 1–11);
- аналіз структур і динаміки показників кібербезпеки, кореляцій, нелінійних зв’язків, аномалій і подієвих патернів на основі емпіричних даних (Теми 3–10);
- робота з офіційними policy-документами у сфері кібербезпеки та кібердипломатії, їх кодування й аналіз із застосуванням підходу text as data (Теми 8, 9).

Інтерактивні методи:

- групова аналітична робота з формування спільного панельного датасету та корпусу документів для семестрового проєкту (Теми 1–5, 8);
- колективний аналіз кореляцій, кластерів, аномалій і подієвих процесів у міжнародній кібербезпеці (Теми 4–10);
- групова підготовка аналітичних візуалізацій і policy-висновків для фінального групового проєкту (Теми 11–14);
- презентація та публічний захист результатів семестрового групового проєкту з кібердипломатії у форматі review (Тема 14).

Методи активізації навчально-пізнавальної діяльності:

- навчання через дослідження (research-based learning) у процесі виконання індивідуальних computational-завдань і семестрового групового проєкту (Теми 1–14);
- проблемно-пошукові завдання, спрямовані на виявлення структурних і динамічних патернів у міжнародній кібербезпеці (Теми 3–7);
- кейс-метод з аналізом конкретних міжнародних кіберінцидентів, дипломатичних реакцій і регуляторних підходів (Теми 5, 7, 10);
- метод проєктів під час виконання семестрового групового завдання Cyber Diplomacy Intelligence Project (Теми 1–14).

ФОРМИ ТА МЕТОДИ ОЦІНЮВАННЯ

Університет використовує 100-бальну накопичувальну систему оцінювання результатів навчання здобувачів вищої освіти.

Поточний контроль здійснюється під час проведення лекційних, практичних (семінарських) занять, і має на меті перевірити рівень підготовленості здобувача вищої освіти до виконання конкретної роботи. Оцінюється сумою набраних балів: для дисциплін з формою семестрового контролю іспит: сума становить 60 балів.

Семестровий контроль проводиться у формах семестрового екзамену (іспиту). Складання семестрового екзамену (іспиту) здійснюється під час екзаменаційної сесії. Максимальна сума балів, яку може отримати здобувач вищої освіти під час екзамену (іспиту) – 40 балів. Мінімальна сума, за якою екзамен (іспит) вважається складеним – 25 балів.

Підсумкова оцінка за навчальною дисципліною визначається шляхом сумування всіх балів поточного контролю та екзамену (максимум – 100 балів).

Для допуску до підсумкового екзамену здобувач повинен набрати не менше 35 балів за поточний контроль. Мінімальна прохідна оцінка за екзамен – 25 балів.

Поточний контроль успішності навчання здійснюється у формі:

- збір, структуризація та первинна візуалізація даних міжнародної кібербезпеки 2 рази впродовж семестру. Максимальна оцінка за одне виконання — 2 бали (*2-бальна система, усього 4 бали*);
- порівняльний аналіз держав у сфері кібербезпеки — 2 рази за семестр. Максимальна оцінка за одне виконання — 3 бали (*3-бальна система, усього 6 балів*);
- аналіз динаміки, кореляцій і структурних вимірів кібербезпеки — 3 рази за семестр. Максимальна оцінка за одне виконання — 3 бали (*3-бальна система, усього 9 балів*);
- аналіз нелінійних зв’язків і аномалій у показниках кібербезпеки — 2 рази за семестр. Максимальна оцінка за одне виконання — 4 бали (*4-бальна система, усього 8 балів*);
- text-as-data аналіз і порівняння кібернаративів — 2 рази за семестр. Максимальна оцінка за одне виконання — 4 бали (*4-бальна система, усього 8 балів*);
- подієвий аналіз кіберінцидентів і дипломатичних реакцій — 1 раз за семестр. Максимальна оцінка — 3 бали (3-*бальна система, усього 3 бали*);

- підготовка індивідуального policy brief або аналітичного огляду — 1 раз за семестр. Максимальна оцінка — 4 бали (*4-бальна система, усього 4 бали*);
- семестровий груповий аналітичний проєкт «Cyber Diplomacy Intelligence Project» — 1 раз за семестр. Максимальна оцінка — 18 балів (*18-бальна система, усього 18 балів*).

Приклад екзаменаційного білета

Харківський національний економічний університет імені Семена Кузнеця

С Соціальні науки, журналістика, інформація та міжнародні відносини

С3 Міжнародні відносини

Перший (бакалаврський) рівень

Семестр II

Навчальна дисципліна «Кібердипломатія»

ЕКЗАМЕНАЦІЙНИЙ БІЛЕТ № 1

Завдання 1 (практичне)

На основі наданого датасету показників міжнародної кібербезпеки (індекси, подієві або панельні дані) виконайте наступне завдання:

а) Обґрунтуйте, який тип аналізу доцільно застосувати до цього датасету (порівняльний аналіз держав / часовий аналіз / кореляційний аналіз / аналіз нелінійних зв'язків / подієвий аналіз) і поясніть свій вибір.

б) Запропонуйте псевдокод або R-логіку для:

- побудови часової динаміки показників кібербезпеки або
- розрахунку кореляцій між індексами кібербезпеки та показниками політичного режиму. (оцінюється логіка аналітичного підходу, а не бездоганний синтаксис)

в) Поясніть, який емпіричний патерн може бути виявлений за допомогою такого аналізу (тренд, асиметрія між групами держав, нелінійна залежність, наявність аномалій тощо).

Максимально — 15 балів за завдання.

Завдання 2 (теоретично-методологічне)

На основі наданого датасету міжнародної кібербезпеки запропонуйте R-код або його структурну логіку для:

- формування панельного датасету у форматі *країна–рік* або

- проведення кластерного чи PCA-аналізу показників кібербезпеки або базового text-as-data аналізу офіційних документів у сфері кібердипломатії.

У відповіді коротко поясніть: які змінні використовуються; яку аналітичну задачу вирішує запропонований код.

Максимально — 15 балів за завдання.

Завдання 3 (евристичне)

а) Поясніть, чому кібердипломатія розглядається як інструмент міжнародної кібербезпеки. Розкрийте логіку взаємодії дипломатії, безпеки та цифрових технологій, наведіть приклади.

б) Поясніть відмінність між: національною кіберполітикою, міжнародною кібердипломатією, глобальним кіберврядуванням.

У відповіді зверніть увагу на акторів, рівні прийняття рішень та інструменти впливу.

Максимально — 10 балів за завдання.

Затверджено на засіданні кафедри міжнародних відносин і політичної філософії, протокол № 1 від «22» серпня 2025 р.

Екзаменатор викл. Непочатов Д. О.

Зав. кафедри д.філос.н., проф. Кузь О.М.

Системи оцінювання, що використовуються, наведено нижче

Критерії оцінювання індивідуальних аналітичних завдань

2-бальна система оцінювання

(базові завдання зі збору, структурування та первинної візуалізації даних)

Ступінь виконання	Бал
Дані зібрані коректно та повністю; структура датасету відповідає вимогам (формат країна–рік, коректні змінні); візуалізації відповідають даним; відсутні критичні помилки.	2
Дані зібрані частково або з помилками; структура датасету порушена; наявні суттєві неточності у змінних або візуалізаціях; завдання виконане формально.	1

3-бальна система оцінювання

(порівняльний аналіз, часові тренди, кореляції, подієвий аналіз)

Ступінь виконання	Бал
Аналіз виконано коректно; дані використано відповідно до завдання; застосовано адекватні методи; результати інтерпретовано логічно; сформульовано короткий аналітичний висновок.	3
Аналіз загалом коректний, але є окремі методичні, технічні або інтерпретаційні неточності; висновки поверхові, однак пов’язані з отриманими даними.	2
Аналіз фрагментарний або формальний; методи застосовано некоректно; інтерпретація слабко пов’язана з даними або відсутня.	1

4-бальна система оцінювання

(кластерний / PCA-аналіз, нелінійні моделі, text-as-data, policy brief)

Ступінь виконання	Бал
Аналіз виконано коректно; застосовано відповідний метод (PCA, кластеризація, LOESS/GAM, text-as-data); код відтворюваний; візуалізації інформативні; результати інтерпретовано аналітично; наявний змістовний висновок.	4
Аналіз загалом коректний; метод застосовано правильно, але інтерпретація частково поверхова або неповна; можливі дрібні технічні неточності.	3
Аналіз виконано частково; метод застосовано формально або з помилками; візуалізації	2

або інтерпретація некоректні.	
Аналіз некоректний або формальний; код не відтворюється; результати не пов’язані з даними або відсутні.	1

Критерії оцінювання аналітичного групового проєкту

18-бальна система оцінювання

Ступінь виконання	Бал
Дані зібрані коректно й повністю; панельний датасет структурований; R-аналіз повністю відтворюваний; використано кілька типів аналізу (порівняльний, часовий, кореляційний, нелінійний, text-as-data або подієвий); аналітичні висновки логічно випливають з емпіричних результатів; фінальний аналітичний документ і презентація демонструють цілісний синтез результатів.	18
Проєкт виконано на дуже високому рівні; дані повні; аналіз відтворюваний; застосовано щонайменше три типи аналізу; інтерпретація коректна, але синтез результатів менш глибокий.	17
Проєкт якісний і структурований; основні етапи аналізу виконані правильно; візуалізації інформативні; аналітичні висновки сформульовані, але частково описові.	16
Проєкт загалом відповідає вимогам; дані зібрані коректно; аналіз виконано, але є окремі технічні або аналітичні недоліки; відтворюваність коду часткова.	15
Проєкт виконано на достатньому рівні; корпус даних обмежений за обсягом або різноманіттям; аналіз коректний, але без глибокого синтезу; зв’язок між даними та висновками простежується.	14
Проєкт демонструє базове розуміння завдання; аналіз фрагментарний; використано обмежену кількість методів; інтерпретація переважно описова.	13
Проєкт виконано частково; дані або аналіз неповні; computational-підхід застосовано вибірково; висновки слабко пов’язані з результатами.	12
Проєкт містить суттєві технічні й аналітичні недоліки; логіка між етапами аналізу порушена; візуалізації або інтерпретація проблемні.	11
Проєкт фрагментарний; дані або код подані некоректно; відтворюваність аналізу відсутня; аналітичні висновки не сформульовані.	10
Проєкт виконано формально; наявні окремі графіки або таблиці без цілісної аналітичної логіки.	9
Проєкт демонструє мінімальне розуміння завдання; дані зібрані частково; аналіз несистемний; висновки декларативні.	8
Проєкт містить серйозні концептуальні та методологічні помилки; дані та аналіз не відповідають завданню.	7
Проєкт фрагментарний і несистемний; більшість обов’язкових компонентів відсутні.	6
Проєкт має ознаки суто формального виконання; аналіз непридатний до інтерпретації.	5
Проєкт майже не відповідає вимогам; подані окремі матеріали без аналітичного зв’язку.	4
Проєкт не відображає змісту завдання; дані та аналіз нерелевантні.	3
Проєкт фактично не виконано; відсутні структуровані дані та аналіз.	2

Подані матеріали не мають змістовного наповнення та непридатні для оцінювання.	1

Критерії оцінювання завдання екзаменаційного білету (практичне)

15-бальна система оцінювання

Ступінь виконання	Бал
Завдання виконано повністю та на високому рівні. Тип аналізу (порівняльний, часовий, кореляційний, нелінійний або подієвий) обрано коректно і чітко обґрунтовано з урахуванням структури датасету міжнародної кібербезпеки. Псевдокод логічний, послідовний, відображає повний цикл аналізу (підготовка даних, агрегація, розрахунок, візуалізація). Емпіричний патерн (тренд, асиметрія, нелінійність, аномалія) описано коректно та пов’язано з обраним типом аналізу.	15
Тип аналізу визначено правильно; обґрунтування загалом переконливе. Псевдокод логічний, але має незначні спрощення або пропуски окремих аналітичних кроків. Емпіричний патерн описано коректно, але інтерпретація менш розгорнута.	14
Тип аналізу підібрано коректно, але обґрунтування частково поверхове. Псевдокод зрозумілий, але поданий у скороченому вигляді. Емпіричний патерн описано загально, без деталізації.	13
Тип аналізу обрано доречно, однак логіка вибору пояснена неповністю. Псевдокод фрагментарний, але демонструє розуміння принципів обробки та підрахунку даних. Емпіричний патерн сформульовано описово.	12
Виявлено часткове розуміння типів аналізу даних міжнародної кібербезпеки. Псевдокод містить логічні неточності або пропущені ключові етапи. Патерн визначено нечітко або без чіткого зв’язку з даними.	11
Тип аналізу визначено формально, без глибокого обґрунтування. Псевдокод схематичний, описує загальну ідею аналізу без чіткої структури. Патерн описано загальними словами.	10
Наявна спроба вибору типу аналізу, але з методологічними неточностями. Псевдокод непослідовний або неповний. Інтерпретація емпіричного патерну слабка.	9
Завдання виконано частково. Тип аналізу визначено некоректно або без пояснення. Псевдокод не дозволяє відтворити логіку аналізу. Патерн сформульовано поверхово.	8
Аналіз і псевдокод подані фрагментарно. Зв’язок між даними, методом і висновками слабкий або відсутній.	7
Формальне виконання завдання. Псевдокод некоректний або не відповідає завданню. Емпіричний патерн не пояснено.	6
Наявні лише окремі елементи відповіді (назва аналізу або загальна ідея підрахунку) без логіки.	5
Спроба відповіді поверхова; суттєві логічні помилки.	4
Завдання виконано неправильно; відсутнє розуміння computational-логіки.	3
Мінімальні, випадкові фрагменти відповіді без змістовного наповнення.	2
Завдання фактично не виконано.	1

Критерії оцінювання завдання екзаменаційного білету (теоретичне)

15-бальна система оцінювання

Ступінь виконання	Бал
Запропоновано коректний і логічно послідовний R-код, який реалізує повний цикл аналізу (вибір змінних, групування, підрахунок, отримання результату). Код узгоджений зі структурою датасету та дозволяє відтворити аналіз.	15
R-код загалом коректний; логіка підрахунку збережена. Наявні незначні синтаксичні або структурні неточності, що не порушують аналітичної ідеї.	14
Код правильний по суті, але поданий у скороченому вигляді (окремі кроки опущено або неявно задано). Принцип агрегації даних зрозумілий.	13
Код правильний по суті, але поданий у скороченому вигляді (окремі кроки опущено або неявно задано). Принцип агрегації даних зрозумілий.	12
Наявне часткове розуміння computational-логіки; код фрагментарний або непослідовний.	11
Код схематичний, описує ідею підрахунку, але не може бути безпосередньо виконаний або відтворений.	10
Подано лише загальний підхід до підрахунку без коректної реалізації у R.	9
R-код містить логічні помилки, що унеможливлюють правильний результат.	8
Формальне виконання завдання; код не відповідає поставленій аналітичній задачі.	7
Наведено окремі R-команди без логічного зв’язку між ними.	6
Мінімальна спроба відповіді; код непридатний до інтерпретації.	5
Суттєві помилки у розумінні принципів аналізу даних.	4
Код не виконує підрахунок згадувань або частот.	3
Випадкові або нерелевантні фрагменти коду.	2
Завдання фактично не виконано.	1

Критерії оцінювання завдання екзаменаційного білету (евристичне)

10-бальна система оцінювання

Ступінь виконання	Бал
Відповідь повна, логічно структурована й концептуально коректна. Пояснено роль кібердипломатії у міжнародній кібербезпеці; використано коректні поняття; наведено релевантні приклади з міжнародної практики.	10
Відповідь аргументована; приклади доречні, але аналітична глибина дещо обмежена.	9
Загалом правильна відповідь; поняття використано коректно, але без розгорнутих прикладів.	8
Виявлено розуміння ключових ідей; аргументація поверхова.	7

Часткове розуміння теми; наявні неточності у визначеннях або прикладах.	6
Часткове розуміння теми; наявні неточності у визначеннях або прикладах.	5
Фрагментарні знання; слабка структура відповіді.	4
Суттєві концептуальні помилки; неправильне розуміння ролі медіа.	3
Мінімальне, поверхове уявлення про тему.	2
Відповідь не відповідає змісту питання.	1

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Основна

1. Міжнародні відносини та світова політика : навч. посіб. / О. М. Кузь та ін. Харків : Харків. нац. екон. ун-т ім. С. Кузнеця, 2020. 200 с. URL: http://repository.hneu.edu.ua/handle/123456789/25295 .

2. Topor L. Cyber sovereignty. Cham: Springer Nature Switzerland, 2024. URL: https://doi.org/10.1007/978-3-031-58199-1

Додаткова

3. Brovko O. Local government resilience in the face of Russian aggression: the case of Ukraine. Territory, Politics, Governance. 2024. P. 1–20. URL: https://repository.hneu.edu.ua/handle/123456789/32772.

4. Kuz O., Konnova N., Korotkov D. Corruption Models of Behaviour in the Structure of the Political System of Society. Dialogue and Universalism. 2024. Vol. 34, no. 1. P. 131–141. URL: https://repository.hneu.edu.ua/handle/123456789/32650

5. Kleiner J. How political regimes affect national cybersecurity: the polity flux effect. Democratization. 2025. P. 1–32.
URL: https://doi.org/10.1080/13510347.2025.2451951

6. Steen S., Janet M B. Cognitive Warfare. Brussels, 2025. 24 p.
URL: https://www.sto.nato.int/document/cognitive-warfare/.

7. Ünver H. A. Computational International Relations What Can Programming, Coding and Internet Research Do for the Discipline?. All Azimuth: A Journal of Foreign Policy and Peace. 2018.
URL: https://doi.org/10.20991/allazimuth.476433

Інформаційні ресурси

8. The World Factbook - The World Factbook. We are the Nation's first line of defense - CIA. URL: https://www.cia.gov/the-world-factbook/
9. Britannica. Britannica. URL: https://www.britannica.com .
10. Atlantic Council. *Atlantic Council*. URL: http://www.atlanticcouncil.org
11. Brookings - Quality. Independence. Impact. Brookings. URL: https://www.brookings.edu