Віктор МАТВІЄНКО,
доктор історичних наук,
завідувач кафедри міжнародних
організацій та дипломатичної служби
Навчально-наукового інституту міжнародних відносин
Київського національного університету
імені Тараса Шевченка;

Ганна ПЕТУШКОВА,
аспірантка кафедри міжнародних
організацій та дипломатичної служби
Навчально-наукового інституту міжнародних відносин
Київського національного університету
імені Тараса Шевченка

КІБЕРДИПЛОМАТІЯ В ЄВРОПЕЙСЬКОМУ СОЮЗІ: МОДЕЛЬ ЕСТОНСЬКОЇ КІБЕРДИПЛОМАТІЇ ТА ДОСВІД УКРАЇНИ

Анотація. У статті йдеться про важливість становлення та розвитку української кібердипломатії з огляду на актуальність цього питання в безпековій площині та за напрямом міжнародної співпраці. Розкрито поняття «кібердипломатія». Порівняно досвід Естонії, а саме Міністерства закордонних справ Естонської Республіки, з наявними можливостями МЗС України. Перелічено положення стратегій кібербезпеки обох держав у питаннях, де передбачено залучення відомств, відповідальних за реалізацію зовнішньої політики. Акцентовано увагу на структурній відмінності зовнішньополітичних відомств обох країн, наявності кадрового потенціалу й успішних ситуаційних кейсах кібердипломатії.

Висловлена думка, що саме Естонію Україна може взяти за зразок для запозичення досвіду становлення кібердипломатії. МЗС України необхідно переглянути підхід до розвитку кібердипломатії. Важливими є її активізація та розширення кола фахівців шляхом долучення дипломатів, які зможуть адаптувати світові практики кібердипломатії до українських реалій.

Ключові слова: кібердипломатія, Естонія, кібербезпека, Україна, стратегія кібербезпеки, Європейський Союз, Посол з особливих доручень з питань кібердипломатії.

Сучасному етапові міжнародних відносин властива нестабільність середовища та поява багатьох викликів і загроз. Серед цього набору виділяється простір із двома онтологічними можливостями, остаточним результатом якого не є конкретний продукт або явище. Йдеться про кіберпростір – живе середовище, яке може бути як безпековим викликом, так і можливістю для розвитку та співпраці.

Важливим з огляду на окреслену проблематику статі розрізняти поняття «цифрова дипломатія» та «кібердипломатія». Якщо ми говоримо про цифрову дипломатію, то йдеться насамперед про застосування цифрових технологій до дипломатії, підтримку дипломатичних ініціатив, полегшення процесів завдяки віртуальним ресурсам. Як приклад – ініціативи зі створення віртуальних посольств чи спрощення консульських послуг для громадян держави за допомогою інтернету. Кібердипломатія – це застосування дипломатії, а саме дипломатичної практики, до кіберпростору. У статті виходимо з розуміння, що кібердипломатію на національному рівні визначають як використання дипломатичних інструментів та ініціатив для забезпечення інтересів держави в кіберпросторі. Завданнями для дипломатичного агента можуть бути: встановлення зв'язку та діалогу між державними і недержавними суб'єктами на різному рівні; запобігання кібергонитві; розбудова глобальних норм у кіберпросторі тощо. Кібердипломатія ґрунтується на вимірах м'якої сили та є ефективною практикою для пом'якшення невизначеності, усунення ризиків і потенційних конфліктів, що походять із кіберпростору. Фундаментальними елементами кібердипломатії є збільшення кіберпотенціалу, зміцнення довіри, дотримання та розвиток кібернорм.

І все ж головні проблеми в кіберпросторі чи в кібербезпеці пов'язані з людським чинником. Здебільшого вони геополітичні. Неузгодженості можна простежити саме на міжнародному та національному рівнях. Виклики кіберпростору – це про успіх перемовин і політичні дебати на тему управління цим середовищем. Одна з головних проблем кібербезпеки – це не про те, як запобігти проникненням, а про політичну мотивацію осіб та організацій узяти відповідальність за регулювання складників кібербезпеки, а також про те, як ці суб'єкти можуть обмежити, притягнути до відповідальності за зловмисну діяльність актора міжнародних відносин. Міжнародне право не може бути застосоване до кіберпростору в повному обсязі та без постійних поправок через швидкий темп розвитку інформаційно-комунікаційних технологій. Наразі світова спільнота має 11 необов'язкових норм відповідальної поведінки держав від групи урядових експертів ООН. Талліннський посібник надає роз'яснення, як застосовувати міжнародне право до кіберпростору. Однак більшість держав має власні концепції та стратегічні плани, що на практиці суперечать

нормам, бо ж ті є необов'язковими. Такі класичні концепції міжнародних відносин, як нейтралітет або контроль над озброєннями, не мають сенсу в кіберпросторі у своїй традиційній формі. У світовій спільноті зростає виклик атрибуції кібератак, а також побутує невеликий острах ескалації між акторами через непередбачені наслідки кіберзлочинів.

У кіберпросторі концепт традиційної дилеми безпеки важко застосувати, оскільки майже неможливо розрізнити наступальні й оборонні операції. Державі А важко виявити намір держави Б, тобто зрозуміти, що є метою проникнення: з'ясувати рівень можливостей захисту, отримати конфіденційну інформацію чи провести один з етапів розвідки перед масштабними кіберопераціями. Крім того, міжнародні організації також зазнають атак із різною метою проникнення. В найближчому майбутньому саме засідання таких організацій зі встановлення й обговорення міжнародних обов'язкових стандартів стануть полем геополітичного бою, оскільки держави просуватимуть власні підходи до управління кіберпростором та його захисту. Тому й важливо залучати дипломатів до глобальної розбудови цього середовища. Набуває значення традиційна дипломатична майстерність – хист виявляти наміри опонента. Наявні підходи окремих регіональних організацій, інтеграційних об'єднань із кібербезпеки демонструють об'єднання друзів, тобто держав з однаковим баченням. У загальній же картині світоустрою всі ці підходи суперечать один одному. Відповідно, потрібно домовлятися з потенційними супротивниками та виробляти спільну візію. Якщо міжнародна спільнота має на меті розширити ефект управління кіберпростором від регіональних, національних ініціатив до глобального уніфікованого підходу, то саме дипломати вибудовуватимуть на основі найкращих практик норми міжнародної поведінки. Із цього контексту випливає потреба вводити в державні структури, відповідальні за зовнішню політику, дипломатів, які розроблятимуть геополітику кіберпростору.

Необхідно зосередитися на переосмисленні ролі дипломатів, реорганізації департаментів і загалом міністерств закордонних справ, щоби задовольнити щораз більшу потребу у фахівцях із питань кібербезпеки в реалізації завдань зовнішньої політики та переосмислити роль нових технологій у сучасних міжнародних відносинах. З огляду на історичні події, пов'язані з кібератаками, а також значний потенціал, підкріплений лідерством серед інших держав у рейтингу з кібербезпеки [1], запропоновано розглянути досвід Естонії, який є лише однією з варіативних моделей можливого розвитку кібердипломатії в Україні.

На початку 2000-х років Естонія першою почала впроваджувати концепцію «e-Residency»: активно просували державну цифрову ідентифікацію, доступ до електронних послуг країни та прозорого бізнес-середовища [2].

Естонія розробила різноманітні опції, зокрема й можливість збирати податки, голоси, дані про стан здоров'я – усе з використанням механізмів онлайн-платформ.

Попри такий інноваційний підхід, 2007 року Естонія зазнала найбільшої у своїй історії кібератаки, оскільки уряд, приватні організації, фінансовий сектор, теле- й радіомовлення та громадяни стали мішенню для російської федерації. 2007 року ще не було ні міжнародного політичного механізму для експертного оцінювання наслідків кібератак, ані процедур звернення по допомогу до інших держав, ані колективного засудження зловмисних кібероперацій. Відтоді Естонія постійно порушує питання кібербезпеки як на двосторонній основі, так і в ООН, ЄС, НАТО, Раді Європи та за їхніми межами. Важливим кроком стало створення 2008 року в Таллінні Об'єднаного центру передових технологій з кібероборони НАТО, де зосереджуються на дослідженні кіберпростору, навчанні, обміні думками, хакатонах та операціях, що охоплюють технічні й нетехнічні складники кіберзахисту. Це мозковий центр, який виробляє рекомендації, проводить конференції та створює екосистему співпраці як для держав-членів, так і для країн, що не входять до НАТО. Україна доєдналася до Об'єднаного центру в Таллінні 16 травня 2023 року. Естонія входить до групи урядових експертів ООН і була учасником вироблення 11 необов'язкових норм відповідальної поведінки держав. Країна має унікальний досвід просування власного бачення кіберпростору на міжнародних майданчиках.

Нині потенціал у кіберсфері вдається значно збільшувати завдяки тому, що загальну безпеку Естонії підтримують НАТО, ЄС, а також добре скоординована діяльність дипломатичного корпусу. Важливо й те, що ідея першого у світі посольства даних була реалізована в Естонії 2015 року. Критично важливі бази даних і сервіси Естонії зберігають у центрі обробки даних високого рівня безпеки в Люксембурзі, що дає змогу забезпечити цифрову стабільність державних органів влади навіть у разі зовнішніх загроз [3].

2018 року МЗС Естонської Республіки створило посаду Посла з особливих доручень із питань кібердипломатії. Остаточне регулювання цього формату забрало приблизно десятиліття з моменту кібератак 2007 року. Восени 2019 року було створено Департамент кібердипломатії під юрисдикцією МЗС Естонської Республіки. 2019 року департамент очолила Амбасадорка з особливих доручень із питань кібердипломатії Хелі Тіірмаа-Клаар [4]. На момент створення штат складався з радників, а також чиновників МЗС Естонської Республіки, які вже мали відповідний досвід. Міністерство і в цей період активно демонструвало солідарність із міжнародною спільнотою щодо атрибуції кібератак. 2018 року воно підтримало вже наявне переконання про долученість російської розвідки до кібератак

«NotPetya» та «WannaCry», спрямованих проти міжнародних організацій, зокрема й Організації із заборони хімічної зброї. Важливо також те, що Естонія чітко визначає обов'язки МЗС у стратегіях кібербезпеки. Третя стратегія кібербезпеки Естонії на 2019–2022 роки мала на меті створити процедуру атрибуції кібератак [5]; відповідно 24 січня 2019 року Уряд затвердив гайдлайн (інструкції і рекомендації) щодо зловмисних кібероперацій, який роз'яснює процедури надання оперативної інформації та контекстуального аналізу. Це необхідно для ухвалення політичного рішення щодо атак. Відповідно до ситуації кожен випадок, а також його негативний вплив, масштаб та інші складники оцінюють окремо. Було створено робочу групу з питань атрибуції, до якої ввійшли представники всіх відповідних міністерств і відомств, зокрема й МЗС.

МЗС Естонської Республіки відповідальне за зовнішню політику та політику ЄС. Відповідно до стратегії на 2019–2022 роки, міністерство в цілі № 3 «Естонія є надійним і сильним партнером на міжнародній арені» визначає як індикатор «щорічну експертну оцінку від МЗС та інших відповідних установ щодо якості змісту та спрямованості міжнародної діяльності Естонії», де йдеться про співпрацю на основі окремих ініціатив через залучення різних структур та інституцій [6, с. 57]. Тому й наголошено на потребі створити цілісний і систематичний огляд механізмів співпраці, що є доречним зауваженням і для України через перевантаженість акторів точковими проєктами. У стратегії наголошено на важливості розвитку кіберкомпетентності акторів через сприяння міжінституційній ротації дипломатів і посадовців та, як наслідок, обміну знаннями. Саме тому «МЗС відіграє важливу роль у цій сфері, оскільки його функція полягає в навчанні дипломатів із питань кібербезпеки та забезпеченні їхньої достатньої кіберкомпетентності, а також розробленні ротації кіберекспертів, які працюють у міжнародних організаціях» [7, с. 59].

Чинним Послом з особливих доручень з питань кібердипломатії Естонської Республіки є відомий експерт із кіберполітики Танел Сепп. Він працює на дипломатичній службі Естонії понад 20 років, маючи за плечима різні країни акредитації – від Бельгії до США, Ефіопії, Афганістану. Якщо розглядати повноваження, то МЗС Естонської Республіки відповідальне за реалізацію кібердипломатії, а до функцій департаменту кібердипломатії належить представлення позиції Естонії в міжнародних і регіональних організаціях, а також сприяння розбудові багатосторонніх і двосторонніх відносин у сферах кібердипломатії, міжнародної кібербезпеки та співпраці з кіберрозвитку. Одним із головних питань є обговорення міжнародного права та розроблення варіантів його застосування в кіберпросторі. Дипломати згаданого вище департаменту опікуються й питанням боротьби з міжнародною кіберзлочинністю та просуванням позиції Естонії щодо

відкритого інтернету. Багато міжнародних делегацій з усього світу щороку відвідує Таллінн, щоб ознайомитися з кібербезпекою Естонії, тому одним із завдань департаменту також є їх прийом і супровід.

Естонія є прикладом держави, яка чітко розуміє важливість навчання державних службовців основ кібердипломатії, що знайшло відображення у створенні Талліннської літньої школи кібердипломатії, яку влаштовують щорічно з 2019 року. Школу організовано в межах Програми багатосторонності та цифровізації у співпраці з МЗС Естонської Республіки, Естонським центром міжнародного розвитку й Академією електронного врядування [8]. Талліннська літня школа кібердипломатії в середньому приймає до 50 осіб із національних державних установ, відповідальних за ухвалення рішень щодо кіберуправління. Здебільшого це дипломати, що розробляють зовнішні кіберполітики. Програма складена англійською мовою, тому кандидатів з інших держав заохочують до навчання. У червні 2023 року проєкт зібрав 53 дипломатів із понад 40 держав. «Основними темами цьогорічної Талліннської літньої школи були: диджиталізація та кібербезпека; міжнародна кібербезпека та відповідальна поведінка держав; забезпечення дотримання рамок кібербезпеки; розбудова кіберпотенціалу та підвищення кіберстійкості» [9]. «Я точно вважаю, що в нас недостатньо дипломатів, які опікуються питаннями кібербезпеки. У багатьох країнах це залежить від спроможності. Отже, як ми можемо допомогти на міжнародному рівні? Наша відповідь – навчити більше дипломатів. Раніше ми зосереджувалися на країнах-однодумцях. Але побачили, що питання спроможності є дуже актуальним у глобальному масштабі. Цього року в нас є учасники з усіх куточків світу», – каже Т. Сепп у подкасті e-Estonia [10]. Посол зазначає, що Талліннська літня школа орієнтована на молодих і перспективних дипломатів, які починають або вже почали роботу над цією темою, але вікова категорія необмежена. Він убачає цифровий розрив у багатьох країнах, де є дипломати «старої школи», які просувають зовнішню політику на основі застарілих підходів 90-х років минулого століття, і є група ентузіастів, що популяризують інноваційні підходи та вказують на важливість цифрової дипломатії та кібердипломатії [11].

Отже, бачимо, що МЗС Естонської Республіки вдало поєднує класичні дипломатичні практики й адаптує їх до сучасних реалій. Результатом цього є створення державної посади Посла з особливих доручень з питань кібердипломатії й окремого департаменту (чого поки що не впроваджено в Україні), а також заохочення до навчання основ кібердипломатії.

Варто зазначити, що аналіз здійснено станом на червень 2023 року з відкритих джерел, маємо констатувати мінімальну кількість даних щодо кібердипломатії в Україні.

Посада Посла з особливих доручень з питань кібердипломатії не є новизною – дедалі більше країн відкривають її при органах зовнішніх зносин, і важливо, що зазвичай це класична державна посада. Тож це сигнал, що певна країна активно опікується цією сферою та зацікавлена в міжнародних процесах, які стосуються тематики кіберпростору. Потрібно акцентувати, що попри самопозиціювання України як держави з великим досвідом у сфері кібербезпеки, МЗС України було б доречно виступати промоутером на світовому рівні щодо потенціалу та роз'яснення інцидентів, а також активно долучатися до міжнародного напрацювання норм. Достатньо подивитися на список представників групи урядових експертів ООН, яка працювала над необов'язковими нормами відповідальної поведінки держав, щоби побачити там Естонію, США, супротивника в кіберпросторі – рф, а також інші держави, але не Україну. Сайт МЗС України наразі надає можливість певною мірою зрозуміти структурне оформлення міністерства. Але попри кількість населення України, розміри території, великий пласт фахових дипломатів і закладів вищої освіти, де готують потенційних міжнародників, МЗС України, на відміну від МЗС Естонської Республіки, не має структурного підрозділу, вузькоспеціалізованого з питань кіберпростору.

Пересічному громадянину важко осягнути, чи є хоча б підрозділ кібердипломатії у межах Департаменту публічної дипломатії та комунікацій, чи все ж таки це підрозділ в Управлінні цифрової трансформації [12]. Так само і з питаннями щодо наявності фахівця на посаді Посла з особливих доручень з питань кібердипломатії. Варто зазначити і брак комунікації назагал щодо стану кібердипломатії в Україні. Таких висновків можна дійти через відсутність інформації про це за запитами на офіційному сайті МЗС України, сторінках у соціальних мережах МЗС України та за гугл-пошуком. Наведемо статистику: станом на 30 червня 2023 року на запит «кібердипломатія Україна» подано 827 результатів, із яких кожен другий лінк мінімально охоплює предмет запиту та не надає розуміння щодо ролі МЗС України в питаннях кібердипломатії, його структуру, фахівців із цього напряму. На запит «Estonia cyber diplomacy» видано 2 010 000 результатів, що фахово описують стан справ кібердипломатії в Естонії, а перший лінк – офіційна сторінка МЗС Естонської Республіки – має на меті ознайомити відвідувачів сайту зі структурою, важливими документами та баченням кібердипломатії МЗС [13]. На запит «Ambassador at Large for Cyber Diplomacy at Ministry of Foreign Affairs of Estonia» надано 163 000 результатів; коли ж проглядати контекст за схожим запитом щодо України, то релевантної інформації немає.

В Україні серед останніх публічних подій, із яких ми можемо дійти хоча б якихось висновків про стан справ у кібердипломатії, є перманентна

участь радника МЗС України з кібердипломатії в Національному кластері кібербезпеки. Отже, видається, що довкола потенціалу та діяльності за напрямом кібердипломатії в Україні створено вакуум інформації. Цю тенденцію аж ніяк не можна аргументувати поняттям «необхідність інформаційної тиші» з огляду на велику активність інших суб'єктів гарантування кібербезпеки (Національного координаційного центру кібербезпеки, Ради національної безпеки і оборони України, Державної служби спеціального зв'язку та захисту інформації України тощо) у їхній міжнародній діяльності, публікаціях в інтернеті, а також зважаючи на інтерв'ю співробітників цих інституцій.

Питання щодо причин такої ситуації в царині кібердипломатії, певно, залишатиметься дискусійним ще якийсь час. Умовно спираючись на часові межі (від активних кібератак 2014 року до середини 2022 року), виокремимо кілька внутрішніх причин:

1. Розмитість понятійно-категоріального апарату, що призводить до зведення до спільного знаменника цифрової дипломатії та кібердипломатії.

2. Затяжне включення МЗС України до суб'єктів гарантування кібербезпеки на основі законопроєкту № 8087, який було зареєстровано лише 29 вересня 2022 року, що, певно, викликає запитання, чому це було зроблено саме тоді, а не раніше.

3. Нечіткий розподіл повноважень між суб'єктами гарантування кібербезпеки, включно з повноваженнями щодо міжнародної діяльності та представлення України у дво- та багатосторонніх форматах.

4. Прогалина в структурі МЗС України – те, що немає вузькоспеціалізованого відділу та постійної комунікації щодо кіберподій.

5. Потенційно низький рівень можливостей і ресурсів для виокремлення кібердипломатії в окрему зону відповідальності та покладання на МЗС України функцій, подібних до тих, що їх виконує МЗС Естонської Республіки, і, не в останню чергу, через розподіл ресурсів, фінансування та дотацій від міжнародних партнерів саме на різні інституції, відповідальні за дії в кіберпросторі, кібероперації та кіберстримування.

З огляду на інформаційну бульбашку, малий відсоток фахівців, залучених до обговорення майбутнього української кібердипломатії, та брак заохочення за вертикаллю згори донизу маємо:

1. Малу кількість людських ресурсів, що потенційно можуть обіймати дипломатичні посади та водночас бути знавцями з кіберпитань.

2. Низький рівень фахового та наукового інтересу саме до кібердипломатії. Такий стан справ спричинений тим, що на тлі інших викликів фахова спільнота ставить цю сферу, в кращому разі, не вище ніж на друге місце в рейтингу першочергових проблем до розв'язання. Додатково цю проблематику зазвичай підсвічує брак майданчиків для обміну думками.

Вважаємо, що кібердипломатія наразі має великий набір можливостей для навчання, майданчиків для дискусій, науково-практичних конференцій тощо. Потрібно мати змогу періодично проводити відкрите обговорення актуальних проблем кібердипломатії за участю експертів, науковців і відповідних інституцій під керівництвом МЗС України. Така ініціатива надаватиме поштовх для обміну ідеями та практиками щодо можливих варіантів розвитку, подолання криз або розбудови співпраці, просування національних наративів на міжнародній арені в царині кібердипломатії.

Звертаючись до Стратегії кібербезпеки України від 2021 року [14], вбачаємо прагнення до партнерства, передусім із ЄС, НАТО, США й іншими державами, на основі взаємодії, в якій одним із пріоритетів є саме європейська та євроатлантична інтеграція у сфері кібербезпеки. Тож за реалізацію цих положень має відповідати МЗС України.

Щодо сфери відповідальності МЗС України, варто зазначити про залучення відомства до завдань згідно з Планом реалізації Стратегії кібербезпеки України від 1 лютого 2022 року [15]. Розглянемо такі завдання.

«Ціль С.3. Ефективна протидія кіберзлочинності

[…]

24. Проводити спільні з ЄС та НАТО заходи, спрямовані на підвищення стійкості в кіберпросторі та спроможності розслідувати, переслідувати кіберзлочинність та реагувати на кіберзагрози. […] *Постійно*» [16].

Наразі це одне із завдань, результати якого можна побачити на практиці. За 2022 рік національні суб'єкти гарантування кібербезпеки з огляду на актуальний стан подій справді активізували всі можливі інструменти для співпраці, використовували різні контакти, жваво проводили дво- та багатосторонні зустрічі з міжнародними партнерами. Однією з головних подій є приєднання України в травні 2023 року до Об'єднаного центру НАТО в Естонії. Держава також постійно контактувала з Агентством ЄС з питань мережевої та інформаційної безпеки. Було проведено кібердіалог зі США в червні 2023 року в Таллінні, українську делегацію очолив заступник Міністра закордонних справ України Антон Демьохін, американську – Посол з особливих доручень з питань кіберпростору та цифрової політики Натаніель Фік із Державного департаменту США.

«Ціль С.4. Розвиток асиметричних інструментів стримування

[…]

29. Посилити заходи щодо забезпечення кібербезпеки інформаційної інфраструктури та кіберзахисту інформаційних ресурсів закордонних дипломатичних установ України та об'єктів державної власності України за кордоном. […] *Перше півріччя 2024 року*

[…]

31. Запровадити гармонізований з євроатлантичною спільнотою підхід до застосування санкцій у відповідь на підривну діяльність у кіберпросторі, розроблення та узгодження з іноземними партнерами механізму спільних дипломатичних та економічних дій і заходів, зокрема запровадження обмежувальних заходів у вигляді економічних санкцій, у відповідь на деструктивну кіберактивність. […] *Друге півріччя 2022 року*» [17].

Результати завдання № 31 не мають значного успіху з кількох причин. По-перше, занадто амбіційно вказано масштаб – «євроатлантична спільнота», бо це складний процес і потрібно працювати майже з кожною країною та її процедурою атрибуції кібератак окремо, а також вивчати можливості накладання санкцій саме через кібератаки. По-друге, ЄС має процедуру спільної дипломатичної відповіді, включно зі змогою запровадити санкції. Європейська рада впровадила режим кіберсанкцій 17 травня 2019 року, ввівши цілеспрямовані обмежувальні заходи щодо кібератак, які можуть загрожувати ЄС або державам-членам. ЄС неактивно використовує цей інструмент дипломатії. Наразі на ресурсі «EU Sanctions Map» за категорією «кібератаки» є згадки про замороження активів і заборону на надання коштів, а також про обмеження на в'їзд до ЄС малої кількості вихідців із різних країн [18].

«32. Застосовувати усі доступні інструменти дипломатії та міжнародного права задля протидії зловмисній діяльності у кіберпросторі проти України. […] *Постійно*

33. Налагодити систематичний обмін інформацією про деструктивну діяльність у кіберпросторі з міжнародними партнерами, насамперед Сполученими Штатами Америки, державами – членами ЄС та державами – членами НАТО, створити платформи такого обміну. *[…] Створення платформ – перше півріччя 2023 року. Реалізація – постійно*» [19].

Загалом положення цілі С.4. мають ефект накопичення дій у часі: кількісні та якісні результати співпраці з партнерами, застосування інструментів дипломатії, створення платформи будуть відчутні, коли конкретні ініціативи та проєкти буде запущено й мине якийсь часовий проміжок.

«Ціль К.2. Професійне вдосконалення, кіберобізнане суспільство та науково-технічне забезпечення кібербезпеки

[…]

62. Залучити суб'єктів національної системи кібербезпеки до міжнародних програм навчання і підвищення кваліфікації персоналу. […] *Постійно*» [20].

Це завдання є важливим для розбудови кадрового потенціалу та підвищення спроможності якомога більшого кола співробітників до обговорення кібертем.

«Ціль В.3. Прагматичне міжнародне співробітництво

[…]

84. Забезпечити участь України у міжнародних заходах ООН щодо заохочення відповідальної поведінки держав у кіберпросторі. […] *Постійно*

85. Забезпечити участь України у доопрацюванні Другого додаткового протоколу до Конвенції про кіберзлочинність щодо вироблення заходів та гарантій для вдосконалення міжнародної співпраці між правоохоронними та судовими органами, а також між органами влади та постачальниками послуг в інших державах. […] *Постійно*

86. Розширити шляхом діалогу з міжнародними партнерами доступ правоохоронних органів України до ресурсів Європейського центру боротьби з кіберзлочинністю, до телекомунікаційної системи Інтерполу 1-24/7. […] *Перше півріччя 2023 року*

[…]

91. Забезпечити розвиток міжнародного співробітництва у сфері кібербезпеки шляхом підтримки міжнародних ініціатив у цій сфері, які відповідають національним інтересам України. […] *Постійно*

92. Продовжити практику проведення двосторонніх кібердіалогів з державами – партнерами з метою обміну передовим досвідом у сфері кібербезпеки, інформацією про кіберзагрози, розвитку комунікації між заінтересованими державними органами України та іноземних держав, розширити коло держав – партнерів, з якими проводяться кібердіалоги, ініціювати питання щодо укладення двосторонніх договорів про співпрацю у сфері кібербезпеки. […] *Постійно*» [21].

Ціль В.3 є найфундаментальнішою, якщо Україна хоче зарекомендувати себе як державу, що може диктувати тенденції регулювання кіберпростору та долучатися до створення норм. Знову стикаємося з питанням потенціалу та компетенцій кадрів, саме тому наразі варто орієнтуватися на становлення групи осіб і підготовку співробітників, які зможуть узяти відповідальність за розробку стратегії та реалізацію кібердипломатії України.

Висновки. Говорити про успіхи української кібердипломатії ще зарано, але ця сфера є доволі амбіційною для подальшого розвитку. Саме тому як один із варіантів запозичення досвіду було запропоновано Естонію з її доробком у сфері кібердипломатії. Загальна структура розподілу повноважень між державними органами та дипломатичні зусилля Естонії роблять її моделлю-прикладом того, як конвертувати досвід у знання, ділитися напрацюваннями з партнерами, розбудовувати оборонний кіберпотенціал та інтегрувати кібертематику в дипломатичну практику.

Концепція кібердипломатії перебуває лише на початковому етапі становлення, і більшості держав необхідно переглянути свої підходи до неї.

Саме Естонію Україна може взяти за первинний прототип. Звичайно, що це має відбуватися з адаптацією до власних ресурсів (як державних, так і приватного сектору) й урахуванням безпекових викликів і амбіцій, чітко визначених у часі. Основною метою української кібердипломатії має стати забезпечення стабільності та надійності кіберпростору, а також участь у розробленні норм щодо стримування, узгодженні процедур атрибуції, міжнародної реакції та наслідків для порушників. Зрозуміло, що із закінченням війни спроби проникнути в українські мережі не припиняться, саме тому МЗС України вже має адаптуватися до нових умов, уміти реагувати на події в українському кіберпросторі та водночас бути гравцем, що зможе просувати власне бачення на міжнародному рівні.

1. *National Cyber Security Index* (no date). Available at: https://ncsi.ega.ee/ncsi-index/?order=-ncsi (Accessed: 24 June 2023).
2. e-Estonia (no date) *This is the story of the world's most advanced digital society.* Available at: https://e-estonia.com/story/ (Accessed: 20 July 2023).
3. Ibid.
4. e-Estonia (2019) *Estonia takes on a major role in cyber diplomacy with a new department for international cooperation.* Available at: https://e-estonia.com/estonia-cyber-diplomacy-international-cooperation/ (Accessed: 24 June 2023).
5. Ministry of Economic Affairs and Communications of Estonia (2019) *Cybersecurity Strategy Republic of Estonia.* Available at: https://www.mkm.ee/media/703/download (Accessed: 26 June 2023).
6. Ibid, p. 57.
7. Ibid, p. 59.
8. Delegation of the European Union to the Kingdom of Lesotho (2023) *Welcome to the Tallinn Summer School of Cyber Diplomacy.* Available at: https://www.eeas.europa.eu/delegations/lesotho/welcome-tallinn-summer-school-cyber-diplomacy_en?s=103 (Accessed: 22 June 2023).
9. e-Governance Academy (2023) *The Tallinn Summer School of Cyber Diplomacy brought together participants from 43 countries.* Available at: https://ega.ee/news/tallinn-summer-school-cyber-diplomacy-participants/ (Accessed: 23 June 2023).
10. Plantera, F. (2023) *Cyber diplomats from all around the globe will soon gather in Tallinn* [Podcast]. 6 June. Available at: https://ega.ee/blog_post/cyber-diplomacy (Accessed: 24 June 2023).
11. Ibid.
12. Структурні підрозділи // Міністерство закордонних справ України. URL: https://mfa.gov.ua/pro-ministerstvo/struktura/strukturni-pidrozdili
13. Ministry of Foreign Affairs of Estonia (2023) *Cyber diplomacy.* Available at: https://www.vm.ee/en/international-law-cyber-diplomacy/cyber-diplomacy (Accessed: 24 June 2023).
14. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України № №447/2021 від 26.08.2021. URL: https://www.president.gov.ua/documents/4472021-40013
15. Про План реалізації Стратегії кібербезпеки України: Рішення Ради національної безпеки і оборони України від 30.12.2021. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text
16. Там само.
17. Там само.
18. *EU Sanctions Map* (2023). Available at: https://www.sanctionsmap.eu/#/main (Accessed: 25 June 2023).
19. Про План реалізації Стратегії кібербезпеки України: Рішення Ради національної безпеки і оборони України від 30.12.2021. URL: https://zakon.rada.gov.ua/laws/show/n0087525-21#Text
20. Там само.
21. Там само.

Viktor MATVIIENKO,
Doctor of History,
Head of the Department of International
Organisations and Diplomatic Service,
Educational and Scientific Institute of International Relations,
Taras Shevchenko National University of Kyiv;

Hanna PETUSHKOVA,
Postgraduate Student,
Department of International
Organisations and Diplomatic Service,
Educational and Scientific Institute of International Relations,
Taras Shevchenko National University of Kyiv

CYBER DIPLOMACY IN THE EUROPEAN UNION: THE ESTONIAN CYBER DIPLOMACY MODEL AND THE EXPERIENCE OF UKRAINE

Abstract. The article discusses cyberspace, a key element in the contemporary international stage, which presents security challenges and opportunities for progressive development and cooperation among nations. The article focuses on two distinct concepts in the realm of international relations: digital diplomacy, an innovative approach that leverages digital technologies to facilitate related processes and achieve strategic initiatives, and cyber diplomacy, a sophisticated framework that employs diplomatic practices in cyberspace to assert and safeguard state interests.

The intricate realm of national and international cyberspace and cybersecurity reveals that the major challenges stem from human behaviour and technical factors. The authors analyse the experiences of the Ministries of Foreign Affairs of Estonia and Ukraine, highlighting structural differences within foreign policy agencies, human resources availability, and effective cyber diplomacy implementation situational cases. Consequently, the conclusion ascertains that Estonia can serve as a model for Ukraine to emulate in terms of adopting and applying successful experiences in establishing cyber diplomacy.

Furthermore, the article addresses the debatable subject of the inactive development of cyber diplomacy in Ukraine. It emphasises the importance of reassessing the vision of the Ministry of Foreign Affairs of Ukraine regarding the advancement of cyber diplomacy and broadening the circle of adept diplomats who can adapt global cyber diplomacy practices to suit Ukrainian realities. The highlighted key points revolve around the necessity to foster cooperation with international partners and create platforms for exchanging ideas on cyber diplomacy issues.

Keywords: Cyber diplomacy, Estonia, cybersecurity, Ukraine, cyber security strategy, European Union, Ambassador-at-Large for Cyber Diplomacy.