МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

ФАКУЛЬТЕТ СОЦІАЛЬНИХ НАУК І СОЦІАЛЬНИХ ТЕХНОЛОГІЙ

КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН

КВАЛІФІКАЦІЙНА РОБОТА

освітній рівень – бакалавр

на тему: **«**Проблеми цифрової безпеки та її значення для дипломатії: аналіз загроз та ризиків**»**

Виконав/ла:
Студент/ка 4 року навчання
Спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»

Сабашенко Марія Сергіївна

Керівник

Гош Мрідула
Доктор філософії, старший викладач

КИЇВ 2023

ЗМІСТ

ВСТУП

Актуальність дослідження. Цифрова безпека та інформаційна безпека розглядається у загальному контексті забезпечення захисту від загроз, пов'язаних з використанням інформаційних технологій та обміном інформацією. Це включає в себе захист персональних даних та інформації, яка зберігається в цифровому вигляді, а також захист від кібератак та зловмисних програм. Інформаційна безпека також охоплює заходи щодо захисту від ризиків, пов'язаних з неправильним використанням та поширенням інформації, такої як фейкові новини та дезінформація. Ці два поняття є взаємопов'язаними і мають важливе значення для захисту інформації та безпеки в цифровому світі. У контексті дипломатичних установ цифрова безпека та інформаційна безпека є надзвичайно значущими аспектами захисту даних та інформації, які можуть мати велике значення для національної безпеки та інтересів держави. Дипломатичні установи забезпечують безпеку та захист даних, що стосуються державних секретів, політичних переговорів, зустрічей, телекомунікацій та інших важливих подій.

У цілому, цифрова безпека в дипломатичних установах є складним процесом, який потребує ретельного планування, постійного моніторингу та оновлення технічних та організаційних заходів захисту.

Проблематика дослідження. Поширення використання цифрових технологій у сучасній дипломатичній діяльності і, як наслідок, поява проблем з забезпеченням конфіденційності та захисту інформації, що може стати перешкодою для ефективної дипломатії та відносин між державами.

Дослідницькі питання: Які конкретні загрози та ризики пов'язані з цифровою безпекою в галузі цифрової дипломатії? Які інструменти та стратегії можуть бути використані для захисту конфіденційної інформації в дипломатичних відносинах? Як можуть бути підвищені рівні захисту та безпеки?

Об'єктом дослідження є цифрова безпека у цифровій дипломатії.

Предметом дослідження є загрози та ризики, пов'язані з використанням цифрових технологій в дипломатичній діяльності.

Мета дослідження визначити ефективні напрями та механізми забезпечення цифрової безпеки та її значення для дипломатії.

У дослідженні було поставлено такі завдання:

- розкрити поняття цифрової безпеки та її значення для дипломатії;
- з'ясувати ризики та загрози для дипломатії у сфері цифрової безпеки;
- виокремити сучасний досвід та практики забезпечення цифрової безпеки в дипломатії;
- систематизувати заходи з забезпечення цифрової безпеки дипломатичних установ України міжнародним стандартам та рекомендаціям;
- встановити важливість забезпечення цифрової безпеки для дипломатії;
- надати пропозиції щодо вдосконалення заходів забезпечення цифрової безпеки в дипломатії.

Дослідження проблеми цифрової безпеки у дипломатії свідчить про значущість інформаційної складової. Практична значимість роботи полягає у можливості використання сформульованих положень, висновків як інструментів та положень для державної політики у сфері інформаційної безпеки. Результати дослідження можуть сприяти подальшому аналізу актуальних проблем цифрової безпеки управління, дослідженням у сфері політології, соціальної комунікації та міжнародних відносин.

Методологічні засади дослідження. Методологію дослідження складає контент аналіз наявної літератури. Методологічна концепція герменевтики використовується для аналізу проблем цифрової безпеки та її значення для дипломатії, оскільки такі поняття як культура, мова та інтерпретація, важливі для розуміння технологічних і соціальних викликів, пов'язаних з цифровою безпекою.

Огляд літератури. Дослідженню питань цифрової дипломатії та цифрової на сьогодні присвячено чимало робіт. Відтак, Макаренко Є., Рижков М. розглядають виклики, які виникають у сфері зовнішньої політики в умовах розвитку інформаційного суспільства та досліджують можливості використання інтернет-технологій для досягнення зовнішньополітичних цілей. Робота Н. Піпченко «Соціальні медіа у структурі зовнішньої політики провідних міжнародних акторів»

розглядає питання використання соціальних медіа у зовнішній політиці країн, таких як США, Великобританія, Франція, Німеччина та росія. Книга зосереджується на тому, як соціальні медіа впливають на зовнішньополітичну діяльність країн, зокрема на їх здатність впливати на громадську думку в інших країнах, залучати до діалогу на міжнародному рівні та просувати свої інтереси. Я.Турчин досліджує використання електронної дипломатії в США та її правову базу. Автор звертає увагу на те, що е-дипломатія стала невід'ємною частиною зовнішньої політики США і дозволяє прискорити процеси прийняття рішень та зменшити витрати. Дослідження також наголошує на важливості забезпечення кібербезпеки в е-дипломатії та використання шифрування для захисту інформації. Автор розглядає деякі випадки порушення кібербезпеки, які сталися в США та вказує на необхідність зміцнення заходів з кібербезпеки. Дер Деріан у своєму дослідженні «Квантова дипломатія» розглядає безпеку для цифрової дипломатії як багатогранний об’єкт, що поєднує технічні, соціальні та політичні аспекти поняття. Автор використовує концепцію квантової дипломатії для пояснення сучасного стану цифрових міжнародних відносин, а концепцію цифрової невизначеності для зображення впливу інформації мереж на поведінку окремих груп і зовнішньополітичну діяльність. Група зарубіжних дослідників, такі як С.Бйола та І.Майнор, М.Бей та С.Бултон у своїх працях знаходять підходи до визначення поняття кібербезпеки та фокусуються на цифрових загрозах. У тому числі робота Н. Лорда аналізує технічні загрози - фішингові атаки, які є наразі поширеними у цифровому просторі, та визначає як можливо їх попередити. Автори Р.Соломон та Т. Ренард аналізують виклики для дипломатії з поширенням інтернет середовища у США та ЄС. Також, у своїх дослідженнях Б.Шварценбах та Н.Весткот зосереджуються на описі впливу соціальних медіа та інтернету на міжнародні відносини та зовнішню політику. У роботі використовуються нормативні документи, такі як «Указ Президента України Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року», Стратегія національної

безпеки України, Стратегія публічної дипломатії Міністерства закордонних справ України, Указ президента України №37/2022 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії кібербезпеки України», Стратегія кібербезпеки Німеччини, США. Наведені нормативні документи та стратегії регламентують засади кібербезпеки в Україні та провідних державах. Для огляду рівня кіберзбепеки у країнах використовувалися статистичні дані з ресурсу National Cyber Security Index.

Структура роботи. Робота складається зі вступу, трьох розділів, висновків до кожного розділу, загальних висновків та списку використаних джерел. Перелік використаних джерел включає 52 найменування.

РОЗДІЛ 1
ТЕОРЕТИЧНІ АСПЕКТИ ЦИФРОВОЇ БЕЗПЕКИ ТА ЇЇ ЗНАЧЕННЯ ДЛЯ ДИПЛОМАТІЇ

1.1. Поняття цифрової безпеки та її значення для дипломатії

Державні органи у сфері зовнішніх зносин зараз активно шукають нові підходи та інструменти для забезпечення національних інтересів. Публічна дипломатія стає все важливішою, оскільки трансформація світової політичної організації підсилює її роль у формуванні іміджу країни. Нова публічна дипломатія орієнтується на концепцію м'якої сили, вступаючи у діалог із суспільствами інших країн та конкуруючи за увагу третіх сторін. Окрім того, використання інтернет-технологій у дипломатії є глобальним феноменом, і він супроводжується зростаючим академічним інтересом до «цифрової дипломатії». Дослідники вивчають практику впровадження цифрових процесів у діяльність посольств, дипломатів, відомств та світових політичних лідерів. Вони наголошують на необхідності усвідомлення державною владою та місцевими спільнотами зростаючого потенціалу інформаційно-комунікаційних технологій в інтерактивному спілкуванні з аудиторією та пошуку точок взаємодії у прийнятті політичних рішень (Піпченко, 2019).

У роботі використовується метод якісного контент аналізу, оскільки за допомогою даного методу можна найкраще оцінити прихований та явний контексти груп документів та літератури, на досліджені яких базується робота. Даний метод дозволяє виокремити закономірності у певних подіях, станах та ставленні лідерів і організацій точки зору з урахуванням їх контексту. Зібрана інформація систематизувалась у тому числі за допомогою методу системного аналізу для того, оскільки такий спосіб надає можливість включити фактори, які можуть впливати на стан досліджуваного об'єкту.

Феномен міжнародної цифрової безпеки є складним явищем, оскільки для його повного зрозуміння необхідно дослідження суміжних термінів, таких як

інформаційний простір та інформаційне суспільство. Деякі експерти наголошують на важливій різниці між цими термінами, які часто використовуються як синоніми. Інформаційний простір – це сукупність інформаційних ресурсів, систем і технологій, які працюють на загальних принципах та структурують взаємодію між людьми. Його складовими елементами є неживі об’єкти та результати людської діяльності. У свою чергу, інформаційне суспільство – це нова фаза розвитку цивілізації, в якій головними продуктами є інформація та знання, а головним елементом – людина (Піпченко, 2015).

Цифрова безпека та інформаційна безпека є поняттями, пов'язаними з захистом даних та інформаційних ресурсів, але вони мають певні відмінності. Цифрова безпека фокусується на захисті цифрових технологій, систем і інфраструктури, охоплює заходи безпеки, спрямовані на захист від кіберзагроз, таких як хакерство, віруси, кібератаки, зловживання даними тощо, займається захистом комп'ютерних мереж, електронних пристроїв, програмного забезпечення та даних, що зберігаються та передаються в цифровій формі. В той час як інформаційна безпека охоплює захист інформації, незалежно від форми або медіа, в якому вона знаходиться (цифрова, паперова, усна тощо), включає політики, процедури і технічні заходи для забезпечення конфіденційності, цілісності, доступності та надійності інформації, та займається не тільки технічними аспектами, але й охоплює людей, процеси, стандарти та культуру організації (Піпченко, 2015).

Також можна виділити три групи дослідників, які наголошують на різних тенденціях тлумачення поняття «цифрова безпека». Хоча й усередині цих груп також виділяються дещо інші погляди цього поняття. Основну увагу при розгляді питань цифрової безпеки приділяють забезпеченню безпеки телекомунікаційних та автоматизованих інформаційних систем, а також інформації, що зберігається та обробляється на персональних комп’ютерах (Карчева, Огородня, Опенько, 2017). Ця тенденція є найпоширенішою в цій групі, але її поява повністю виправдана та викликана низкою факторів, включаючи наступні:

- електронні засоби обробки, передачі, накопичення та зберігання інформації є основою більшості сучасних інформаційних технологій;
- технічні засоби, що призначені для негласного отримання інформації, здобули широке поширення і на початковому етапі не зазнали належної протидії;
- право щодо цифрової безпеки має суперечливий та недосконалий характер;
- недостатня кількість фахівців гуманітарного профілю (насамперед юристів) з даної проблематики;
- та нестача комплексних розробок з проблем забезпечення інформаційної безпеки, які залучають фахівців як гуманітарного, так і технічного профілю (Riordan, 2016).

Хоча підвищена прозорість може мати більш очевидні ефекти в дипломатичних сферах, її протилежна умова – нестабільність – проявляється більш яскраво в галузі безпеки. Як то в контексті кібербезпеки, так і в кризових ситуаціях, нестабільність негативно впливає на національну безпеку на всіх рівнях – від стратегічного до практичного. Як показують дослідження А. Каспер та В. Вернігова, зброя проти масштабної нестабільності змінилася на непередбачувані кризи, що вимагають політичних та соціальних рішень (Kasper, Vernigora, 2021). Тоді як проблеми безпеки, які раніше формулювалися як лінійні та виміряні з передбачуваними масштабованими рішеннями, сьогодні виглядають хаотичними, випадковими та непередбачуваними. Хоча загрози зосереджені на людині та вимагають інноваційних та нетрадиційних рішень, національна політика безпеки не досягла рівня, де може передбачати та управляти цим станом, а не реагувати на нього як постійну умову (Карчева, Огородня, Опенько, 2017).

Сучасна епоха вимагає нових інструментів та підходів до дипломатії, які зосереджені на певних аспектах, таких як вірогідний вплив, участь та стійкість. С. Ріордан аргументує, що для досягнення цих цілей необхідно розглядати безпеку в більш широкому контексті, не тільки як війну або технічне переважання (Riordan, 2016). У цьому контексті політика цифрової безпеки може виступити каталізатором для потрібної дискусії про зміни. Розв’язання проблем цифрової безпеки потребує

інтеграції різних питань, таких як оборонні можливості, приватність, громадянські свободи, довіра громадськості, свобода Інтернету та глобальне управління, а також фокусуванні на швидкості змін. Це охоплює значну частину нестабільності, яку сьогодні повинна вирішувати національна політика безпеки (Малюта, Дерманська, 2019).

Цифрова безпека має велике значення для дипломатії, оскільки дипломатична діяльність передбачає обмін конфіденційною інформацією, яка може стати легкою мішенню в онлайн-середовищі. Незадовільний захист цієї інформації може мати серйозні наслідки, такі як порушення міжнародних угод, підрив довіри між країнами, або навіть загроза національній безпеці. Зазвичай ця інформація містить важливі дані про національну безпеку, зовнішню політику, економіку та інші секретні дані, що потребують високого рівня захисту (Ruffini, 2017).

Для забезпечення безпеки конфіденційної інформації в дипломатії важливо використовувати різноманітні технічні засоби та заходи. Ці засоби включають захист мереж та серверів, використання шифрування, рівень доступу, системи ідентифікації та аутентифікації, віддалений моніторинг та аналіз. Додатково, цифрова безпека також важлива для захисту державних інформаційних систем від кібератак. Це є необхідним для забезпечення безпеки інфраструктури, економіки та соціально-політичної стабільності країни (Карчева, Огородня, Опенько, 2017).

Отже, захист державних інформаційних систем від кібератак є надзвичайно важливим, оскільки такі системи містять значну кількість інформації про національну безпеку та зовнішню політику. Для забезпечення цифрової безпеки в дипломатії можуть бути використані різноманітні технічні та організаційні заходи, такі як сучасні системи захисту від кібератак, які забезпечують відстеження та блокування потенційних загроз, шифрування даних, визначення та контроль рівнів доступу, моніторинг системи та інші.

1.2. Ризики та загрози для дипломатії у сфері цифрової безпеки

Розглянемо три основні підходи, якими держави забезпечують безпеку інформаційного простору та зберігають її:

- зміцнення власного захисту для попередження та захисту від потенційних кіберзагроз;
- стримування інших суб'єктів, як державних, так і недержавних, від участі у свідомо небезпечній діяльності, пов'язаній з аналізом, обробкою та передачею інформації;
- публічна дипломатія для захисту власних національних інтересів та цінностей на міжнародній арені (Field, 2016):

Співіснування дипломатичних відомств і суспільства у новому форматі тісної взаємодії призводить до того, що сучасна дипломатія стає більш інтегрованою до суспільних реалії. В цьому контексті, дуже важливо застосовувати нові засоби комунікації з їхнім унікальним стилем спілкування та зберігати інформаційну ініціативу, щоб запобігти зниженню рівня політичної культури, подібно до дипломатичного відомства рф та інших країн. Використання цифрових технологій у дипломатичній сфері відкриває нові можливості для здійснення політики «м'якої сили», досягнення консенсусу та подолання політично-соціальних та економічних криз, а також вироблення заходів щодо їх запобігання (Riordan, 2016).

Для забезпечення цифрової безпеки в публічній дипломатії необхідно мати розуміння технологічних можливостей та потенційних ризиків зловживання ними. Останнім часом практика дипломатії охопила нові аспекти політики, включаючи проблеми, пов'язані з цифровою трансформацією (Riordan, 2016).

Відтак з поширенням цифрового простору публічна дипломатична діяльність стає все більш інтенсивною. Національні інтереси визначаються в межах стратегій розвитку цифрового простору та інформаційної безпеки, а також у контексті зовнішньої політики в галузі цифрових технологій (Ruffini, 2017). Застосування цифрових інструментів є додатковим викликом, але в той же час вони можуть бути корисними для досягнення цілей у сфері публічної дипломатії (Riordan, 2016).

У контексті публічної дипломатії, головними завданнями забезпечення цифрової безпеки є:

- здійснення відповідальної поведінки держав у цифровому просторі на міжнародному рівні та зміцнення взаємної довіри;
- захист цифрової інфраструктури та Інтернет-простору від зовнішніх загроз;
- запобігання конфліктам у цифровому просторі;
- розробка та виконання політичних заходів з метою забезпечення мережевої та інформаційної безпеки;
- боротьба з кіберзлочинністю та надання взаємної правової допомоги на міжнародному рівні;
- розробка та реалізація зовнішньої політики в цифровому просторі (Kurbalija, Hone, 2021).

Для вирішення цих завдань необхідно скласти зусилля на всіх рівнях внутрішньої структури держави (Kasper, Vernigora, 2021). На рівні осіб, відповідальних за публічну дипломатію, важливим є підвищення рівня знань та компетенцій, включаючи основне розуміння функціонування Інтернету, а також більш глибоке розуміння ключових питань та стратегічних цілей у сфері політичної та соціально-економічної діяльності держави. Крім того, важливим є розвиток гнучких навичок ведення переговорів. На рівні компаній особливу увагу необхідно приділити питанням забезпечення цифрової безпеки в контексті зовнішньополітичного курсу. Для успішного розв’язання цих завдань потрібна консолідація людських і фінансових ресурсів. Крім того, важливо створити внутрішню культуру неперервного професійного зростання і продвиження по службі, зокрема шляхом підвищення кваліфікації та розвитку цифрових навичок (Малюта, Дерманська, 2019).

Для розробки інституційної та державної політики у сфері цифрового простору, необхідно проводити періодичний моніторинг технічних, правових та економічних аспектів використання цифрових технологій і застосовувати отримані результати (Турчин, 2013).

На міжнаціональному рівні необхідне формування стратегічного розуміння національних, регіональних та глобальних пріоритетів держави фахівцями, оскільки стикаючись з загрозами цифрової безпеки в сфері публічної дипломатії, держави потребують компетентності у цьому питанні.

Зокрема, такі загрози визначені фахівцями М.Касснер (2019), Д.Памент (Pamment, 2016), С.Ріордан (Riordan, 2016):

1. Зростаючий рівень свободи в Інтернеті та соціальних мережах: в даний час створення веб-сайтів міністерствами закордонних справ, посольствами та делегаціями міжнародних організацій є стандартною практикою. Веб-сайти міністерств закордонних справ є засобом для пояснення та представлення національної зовнішньої політики та для спростування неприйнятних дій або претензій інших держав (якщо такі виникають). Однак, соціальні мережі є більш відкритими та прозорими платформами.

Інформаційна глобалізація сприяє формуванню цифрових зв'язків та співпраці, що включає публікацію експертних та аналітичних оглядів зі зіткненням інтересів. Однак, доступність Інтернету може бути використана зі злочинними намірами: терористичні та націоналістичні організації використовують Інтернет для мобілізації та набору нових членів, поширюються ідеї екстремізму та насильства. Інтернет-майданчики дозволяють збільшення впливу на розробку міжнародних та внутрішньонаціональних політичних проектів, що може призвести до складнощів у контролі цих процесів (Pamment, 2016).

2. Необхідно розглянути проблему швидкого застаріння знань та компетенцій у цифровому просторі. Для міністерств закордонних справ на сьогоднішній день важливо забезпечити своєчасне навчання дипломатів в ефективному використанні цифрових засобів зв'язку, а також призначити відповідальних осіб для аналізу та вивчення передових науково-технічних досягнень (Ruffini, 2017), які в подальшому можна буде впроваджувати у дипломатичну діяльність.

3. Активне використання інтернет-технологій та соціальних мереж є безпосереднім викликом для збереження секретності в публічній дипломатії через загрозу розкриття інформації. Органи державного управління повинні негайно

поширювати інформацію про відбувшуся подію, але це також може стати ризиком. Незважаючи на це, комунікаційна культура в соціальних мережах залишається досить низькою, що часто веде до образ і провокаційних повідомлень для політичних лідерів і дипломатів, що збільшує ризик виникнення розбіжностей. Тому державні органи, дипломати та представники громадянського суспільства повинні координувати зусилля з метою етичного та нормативно-правового регулювання цифрового простору (Riordan, 2016).

4. Культура анонімності є ще однією серйозною загрозою цифрової безпеки публічної дипломатії. Недостатнє дотримання етичних принципів та практик у віртуальному просторі може призвести до публікації конфліктогенної та неправдивої інформації, що може призвести до виникнення серйозних кризових ситуацій (Карчева, Огородня, Опенько, 2017).

5. Хакерство становить один з найбільш серйозних ризиків цифрової безпеки у сфері публічної дипломатії. Хакерські атаки можуть спричинити значні збитки та погрожувати кар'єрі та місії глав держав, представників урядових та неурядових організацій та дипломатів. Дипломатичні суперники, включаючи як державні, так і недержавні організації, активно намагаються здійснювати атаки на урядові системи країн з метою отримання конфіденційної стратегічної інформації (Ruffini, 2017).

Дипломатія може грати важливу роль у захисті та стримуванні, наприклад, шляхом використання дипломатичного сигналінгу для демонстрації ризиків відповіді опонентам. Однак, дипломатія також може внести вагомий внесок у зміцнення міжнародної кібербезпеки разом з заходами захисту та стримування. Важливою відмінністю є те, що заходи захисту та стримування, ймовірно, можуть бути ефективнішими в короткостроковій перспективі, в той час як дипломатія є найбільш перспективним інструментом для підтримки міжнародної кібербезпеки та забезпечення стабільності у довгостроковій перспективі (Riordan, 2016).

Хоча заходи захисту та стримування мають майже безпосередні позитивні ефекти на кібербезпеку держави, вони несуть ризик продовження ескалації. Постійні інвестиції в інструменти захисту можуть спричинити «кіберзбройну гонку» між потенційними опонентами, а незначні події можуть ескалюватися до

небезпечного циклу «відповідь-на-відповідь» з посиленням серйозності через зусилля з відповіді на ефективне стримування (Graham, 2020).

Найважливіший внесок, який дипломатія може зробити для міжнародної кібербезпеки, полягає у міжнародних нормах. Прийняті міжнародні норми можуть покращити міждержавну співпрацю, прозорість та передбачуваність з метою зменшення ризиків неправильного сприйняття, ескалації та конфлікту, пов'язаних з кіберзагрозами (Bay, 2016).

Міжнародні норми, встановлені мультилатеральною дипломатією в більшості «невидимі», проте вони дуже впливають на міжнародну безпеку та стабільність. Глобально спільні норми проти використання ядерної зброї, наприклад, роблять її використання практично неможливим вже багато десятиліть. Дипломатія може сприяти створенню подібних норм щодо агресії у кіберпросторі. Норми можуть забезпечувати загальні розуміння між державами, дозволяючи їм розглядати загальні інтереси, а також знаходити способи вирішення конфліктів. Крім того, міжнародні норми сприяють співпраці між державами через спільні цілі та термінологію (Пантєлєєва, 2020).

Дипломатичний шлях встановлення міжнародних норм щодо кібербезпеки не є короткостроковим процесом. Щоб прийти до широко прийнятих норм, потрібно знайти спільні цінності; держави повинні сприймати, що дотримання норм у їх власному національному інтересі. Однак наразі багато держав мають досить різні цінності щодо поведінки держав у кіберпросторі. Особливо різні інтереси стосовно цінності відкритої та вільної Інтернет-мережі та визначення кібербезпеки ускладнюють встановлення міжнародних норм. Крім того, держави не можуть самостійно встановлювати норми щодо кіберпитань (Карчева, Огородня, Опенько, 2017).

Слід зазначити, що міжнародні норми не мають юридичної обов'язковості, тому їх успішність повністю залежить від довіри між державами, які беруть участь. Юридично обов'язкові інструменти, такі як договори або конвенції щодо поведінки держав у випадках кіберагресії, здаються нереалістичними в поточній ситуації, не лише через відсутність спільних поглядів між державами, але і через труднощі у

перевірці виконання юридично обов’язкових інструментів щодо поведінки в кіберпросторі. В епоху цифровізації надзвичайно важливим стає реалізація методів контролю інформації та забезпечення інформаційної безпеки, і цей напрямок займає центральне місце у міжнародних дипломатичних та політичних програмах провідних політичних та дипломатичних об’єднань світу.

1.3. Сучасний досвід та практики забезпечення цифрової безпеки в дипломатії

Традиційно на міністерства закордонних справ було покладено завдання врегулювати відносини дружби та ворожнечі з іншими державами, тоді як дипломатична комунікація бачила взаємодію між дипломатами та іноземними сторонами. Проте глобалізація та цифровізація стерли межі між зовнішнім і внутрішнім. У глобалізованому світі неможливо легко відокремити вітчизняне від іноземного, оскільки місцеві проблеми, такі як зміна клімату, тероризм чи навіть зайнятість, вимагають регіональних чи глобальних рішень (Малюта, Дерманська, 2019).

Цифровізація ще більше стирає різницю між внутрішнім і зовнішнім, оскільки міграція громадян на цифрові платформи створює нові можливості для дипломатів згуртувати національну громадську підтримку досягнень зовнішньої політики або схилити громадську думку на користь обраної політики. З точки зору соціальної інформатики, чим більше цифрові технології стирають межі між зовнішнім і внутрішнім, тим більше МЗС доведеться стикатися з проблемами щодо того, чи зможуть вони продовжувати ефективно виконувати свою роботу, не беручи участь у публічних дискусіях на внутрішньому рівні (Riordan, 2016).

Цифрове розмивання зовнішнього та внутрішнього може бути найкраще охоплено концепцією внутрішньої цифрової дипломатії, яка стосується використання цифрових платформ урядами для підтримки своєї зовнішньої політики. На національному рівні групи інтересів та учасники (такі як профспілки та групи активістів) переслідують свої інтереси, чинячи тиск на уряд, щоб він

ухвалив сприятливу політику. На міжнародному рівні уряди намагаються протистояти тиску своїх внутрішніх учасників, водночас мінімізуючи можливий негативний вплив зовнішніх подій. Р.Патнем стверджував, що «політичні складнощі для гравців у цій дворівневій грі є приголомшливими», оскільки лідери повинні йти по канату між внутрішніми та зовнішніми вимогами (Putnam, 1988).

Однак, з іншого боку, цифрові технології можуть також бути використані для перешкоджання дипломатії. Наприклад, Інтернет може бути використаний для поширення дезінформації та фейкових новин, що може спричинити відторгнення дипломатичних домовленостей громадськістю і, нарешті, призвести до їх невиконання. Таким чином, застосування цифрових технологій в публічній дипломатії має свої переваги та ризики, і державні органи мають бути обережні та розуміти їхні наслідки (Bjola, Manor, 2018).

Оскільки оцифрування різко збільшило здатність онлайн-акторів протидіяти урядовій комунікації, Бйола та Манор очікують, що проблема внутрішньої цифрової дипломатії стане більш актуальною в найближчі роки. Міністерства закордонних справ, ймовірно, зіткнуться зі зростаючим попитом на моніторинг активності іноземних опонентів у внутрішньому публічному просторі, картографування їхніх аргументів і спростовування їх майже в реальному часі (Bjola, Manor, 2018).

Часом може статися й протилежне, оскільки внутрішня публічна дипломатія призводить до зовнішніх хвильових ефектів. Одним із класичних прикладів є «селфі», опубліковане колишньою першою леді Мішель Обамою в 2014 році. «Селфі» зображувало першу леді, яка тримала табличку з хештегом «Поверніть наших дівчат», що згадує про викрадення понад 270 нігерійських школярок Боко Харам. Можливо, цей твіт був спробою привернути увагу громадськості США до тяжкого становища викрадених дівчат. Проте за кілька годин після публікації твіту було розпочато протидію кампанії з опублікуванням «селфі» з хештегом «Поверніть свої дрони» та посиланням на прихильність адміністрації Обами до ударів безпілотників (Bjola, Manor, 2018).

Цей приклад не унікальний, а скоріше притаманний цифровим комунікаціям, оскільки онлайн-публіка може приймати або відхиляти дипломатичні повідомлення, що призводить до хвильових ефектів як на внутрішньому, так і на зовнішньому рівнях. Щоб подолати це обмеження, дипломати повинні продовжувати використовувати цифрові інструменти для залучення громадськості та онлайн-розмов. Дійсно, сила цифрових інструментів полягає не в їхній здатності поширювати повідомлення, а в тому, щоб підтримувати та розвивати стосунки через змістовний діалог (Малюта, Дерманська, 2019).

У США існують різні практики та ініціативи для забезпечення цифрової безпеки. У США діє законодавство, спрямоване на забезпечення цифрової безпеки. Комітет з національної безпеки США (National Institute of Standards and Technology (2023) розробляє стандарти та рекомендації з цифрової безпеки, такі як Федеральний стандарт обробки інформації (Federal Information Processing Standards – FIPS). Також існує законодавство, таке як Закон про кібербезпеку (Cybersecurity Act), яке спрямоване на підвищення рівня захисту інформаційних систем.

Велика Британія навчає цифрові підрозділи в МЗС балтійських країн, щоб вони також могли відстежувати та нейтралізувати кампанії з дезінформації. У майбутньому дипломати можуть ще більше сприяти цифровій стійкості своєї країни, працюючи з іншими міністерствами над програмами цифрової грамотності, які допомагають громадянам виявляти небезпечний цифровий контент (Малюта, Дерманська, 2019).

Німеччина відіграє важливу роль у забезпеченні цифрової безпеки та захисті критично важливих інформаційних систем. Країна розробляє та впроваджує різноманітні практики та стратегії, спрямовані на ефективний захист від кіберзагроз. У Німеччині існує Національна стратегія кібербезпеки, яка визначає стратегічні цілі та пріоритети держави щодо цифрової безпеки. Ця стратегія передбачає впровадження комплексного підходу до кібербезпеки, включаючи захист критично важливої інфраструктури, протидію кібершпигунству та кібератакам, забезпечення кібербезпеки громадян і підприємств, а також підвищення кіберсвідомості населення. Німеччина має законодавство, спрямоване

на забезпечення цифрової безпеки. Зокрема, існує Закон про кібербезпеку, який встановлює вимоги до захисту інформації та кіберінфраструктури. Державні органи та регулятори виконують роль нагляду й контролю за додержанням цих вимог. Варто зазначити, що у Німеччині розвинута кіберпромисловість, що сприяє забезпеченню цифрової безпеки. Країна має сильну базу технологічних компаній, які спеціалізуються на кібербезпеці (Cyber Security Strategy for German, 2021).

На міжнародному рівні дипломати можуть створювати коаліції з технологічними компаніями, організаціями громадянського суспільства та неурядовими організаціями, щоб створити «надійне цифрове середовище», у якому учасники розділять тягар ідентифікації та нейтралізації кампаній дезінформації.

Ще одним прикладом з сучасного досвіду забезпечення кібербезпеки є проєкт ініційований НАТО під назвою «Tallin Manual 2.0». Це є другим аналізом від Центру передового досвіду спільної кібероборони НАТО, у якому вчені правничих наук дослідили застосування різних систем міжнародного права у цифровому просторі. Проєкт окреслює кордони державного суверенітету над кібертсруктурою, розглядає права і обов’язки держав, що виникають з суверенного кіберпростору. Відтак, порушення прав та атаки на кіберпростір міністерства чи посольства прирівнюється до порушення суверенітету країни та зазіхання на дипломатичний імунітет, що є повністю неприйнятним у міжнародних відосинах. У аналізі окреслюється така суверенна відповідальність за свої дії, яку мають нести усі учасники (як держави, так і організації) у глобальному спільному кіберпросторі (Michael N. Schmitt Ed., 2013).

Висновок до розділу 1

1. Розробка та прийняття цифрових ініціатив є серйозним викликом для сфери дипломатії, оскільки вони різко змінили розвиток дипломатичної діяльності, аспекти управління та контролю інформації, проведення міжнародних переговорів та врегулювання криз. В той же час, цифрові технології дозволяють збирати та обробляти інформацію про дипломатичну діяльність та забезпечувати оперативний зв'язок у надзвичайних ситуаціях, а також надають можливість громадянам, які живуть у країнах з авторитарним режимом, висловлювати свої думки без обмежень.

2. Попри те, що цифрові технології є надзвичайно корисним інструментом для збору та обробки інформації про дипломатичну діяльність та оперативного зв'язку в надзвичайних ситуаціях, активна діяльність у цифровому просторі також містить значні ризики для публічної дипломатії. Свобода, яка існує в Інтернеті та соціальних мережах, відкриває широкі можливості для кожного, але також може призвести до серйозних проблем. Багато урядів країн світу критикують цифрові платформи за недостатню участь у боротьбі з екстремізмом, тероризмом та антидемократичними ідеологіями, оскільки на їхніх майданчиках може бути будь-яка інформація від будь-якої особи.

3. Представникам дипломатичних організацій необхідно мати знання щодо використання цифрових технологій, Інтернету та соціальних медіа, щоб уникнути негативних наслідків. Розвиток вітчизняних інтернет-майданчиків та платформ з цифровим захистом та збереженням даних, а також застосування технологій інтернет-краудсорсингу можуть бути ефективними заходами для забезпечення цифрової безпеки в сфері публічної демократії, що дозволяють поширювати достовірну інформацію користувачам.

РОЗДІЛ 2
ПРАКТИЧНІ ОСОБЛИВОСТІ ЦИФРОВОЇ БЕЗПЕКИ В ДИПЛОМАТИЧНИХ УСТАНОВАХ УКРАЇНИ

2.1. Аналіз відповідності рівня цифрової безпеки в дипломатичних установах України

З відокремленням від Радянського Союзу та прийняттям незалежності України з'явилась проблема створення позитивного іміджу та бренду країни як важливого учасника міжнародних відносин. У ході наступних років, Україна вдавалась до численних зусиль і затрат на публічну дипломатію, проте діджитал-аспект зайняв своє місце тільки недавно. Зараз інструменти цифрової дипломатії стали ключовим елементом зовнішньополітичної діяльності України в міжнародних відносинах. Аналіз відповідності рівня цифрової безпеки в дипломатичних установах України є важливим завданням, оскільки це дозволяє оцінити стан безпеки інформації в державних органах, забезпечити її захист та запобігти можливим кібератакам та іншим загрозам. Для аналізу рівня цифрової безпеки в дипломатичних установах України можуть використовуватися різні методики, такі як оцінка захищеності інформації за допомогою різних критеріїв, аудит безпеки інформації, пенетраційні тести, а також оцінка реалізації заходів забезпечення безпеки на рівні організації та персоналу (Малюта, Дерманська, 2019).

Період між 2015 та 2016 роками можна вважати новим етапом цифрової дипломатії в Україні. За цей період було створено Управління публічної дипломатії, яке зайнялося ребрендингом офіційних акаунтів МЗС в соціальних мережах та створенням сторінок посольств на платформах нових медіа. У зв'язку з викликами, що виникали на той час, такими як гібридна війна з російською федерацією на міжнародному рівні, МЗС реформувалося та створило новий структурований підрозділ, який мав займатися винятково ключовими

проблемними аспектами функціонування цифрової дипломатії в Україні (Карчева, Огородня, Опенько, 2017).

Загалом, розвиток вітчизняної цифрової дипломатії зазнав стрімкого прогресу в результаті російської агресії в 2014 році, яка мала на меті дестабілізувати Україну та підривати довіру та імідж країни на непідконтрольних територіях так званих ДНР, ЛНР та анексованого Криму. Управління публічної дипломатії запровадило практику синхронних онлайн-кампаній у соціальних мережах українських посольств, які тривають від кількох тижнів до місяця (або більше), з метою одночасного розміщення матеріалів на сторінках Посольств у Twitter та Facebook, які передають ключові меседжі МЗС до іноземних аудиторій щодо збройної агресії рф, боротьби України за власну незалежність, туристичний, науковий, інвестиційний потенціал тощо (Краснопольська, 2022).

Одним з основних критеріїв для оцінки рівня цифрової безпеки в дипломатичних установах України є наявність та використання захисних технологій, таких як антивірусні програми, системи виявлення вторгнень, захищені канали зв'язку тощо. Також важливою є організація робочих місць та інфраструктури, зокрема наявність резервного копіювання даних та систем, контроль доступу до конфіденційної інформації, забезпечення надійності паролів та ідентифікаційних засобів. Додатковою складовою аналізу є оцінка рівня компетентності персоналу в галузі кібербезпеки, їхніх знань про загрози та заходи забезпечення безпеки, а також їхньої готовності до реагування на можливі інциденти та відновлення роботи систем після них (Riordan, 2016).

Наявність відповідних заходів забезпечення безпеки, компетентного персоналу та захисних технологій є важливими складовими для запобігання кібератакам та іншим загрозам, які можуть нанести шкоду державній безпеці. Для покращення рівня цифрової безпеки в дипломатичних установах України можуть бути запроваджені різні заходи, такі як підвищення кваліфікації персоналу в галузі кібербезпеки, оновлення захисних технологій та організації інфраструктури, відновлення резервних копій даних та систем, використання захищених каналів зв'язку та інших заходів. Крім того, важливою складовою є розробка та виконання

програми дій забезпечення цифрової безпеки в дипломатичних установах України, яка включатиме в себе не тільки заходи щодо запобігання кібератакам, а й дії у разі їхнього виникнення, зокрема процедури реагування на інциденти та відновлення роботи систем після них (Малюта, Дерманська, 2019).

Забезпечення цифрової безпеки в дипломатії є надзвичайно важливою та складною задачею. Оскільки дипломати ведуть комунікацію з представниками інших країн та обмінюються чутливою інформацією, вони можуть стати метою кібератак та шпигунства. Для протидії можуть бути використані системи на основі наступних засобів забезпечення цифрової безпеки дипломатії:

Криптографія – використання шифрування для захисту конфіденційної інформації від несанкціонованого доступу. Дипломати використовують криптографію для захисту своїх електронних повідомлень та документів, які надсилаються іншим дипломатам та владі. Криптографічні методи дозволяють шифрувати дані, що забезпечує їх конфіденційність. Також можуть використовуватися цифрові підписи, які підтверджують автентичність повідомлення та документів. У світі дипломатії використовуються різні криптографічні протоколи та системи. Одним з найпоширеніших протоколів є Pretty Good Privacy (PGP), який широко використовують для шифрування та підпису електронних повідомлень (Riordan, 2016).

Безпечні мережі – це ті, що використовуються для передачі даних, включаючи мережі Інтернет, Wi-Fi та внутрішні мережі.

Аутентифікація та авторизація – забезпечення безпеки доступу до ресурсів та систем шляхом перевірки ідентифікаційних даних та надання відповідних дозволів.

Контроль доступу – забезпечення захисту від несанкціонованого доступу до комп’ютерних систем та даних шляхом регулювання прав доступу до них.

Захист від шкідливого програмного забезпечення та від шкідливих програм, які можуть використовуватися для злому дипломатичної інформації (Малюта, Дерманська, 2019).

Ось кілька загальних критеріїв, які використовуються для оцінки стану цифрової безпеки

– Рівень захищеності інфраструктури.

Цей критерій оцінює ступінь захищеності інформаційної інфраструктури від кіберзагроз. Він включає оцінку наявності технологічних заходів безпеки, систем виявлення та реагування на інциденти, а також політик і процедур безпеки. Оцінка ступеня захищеності інформаційної інфраструктури від кіберзагроз в Україні вимагає комплексного аналізу різних факторів технічного, організаційного та процедурного характеру. Офіційні дані щодо точного стану захищеності інформаційної інфраструктури в Україні обмежені, оскільки це питання стосується національної кібербезпеки. Україна має національний орган з питань кібербезпеки – Державну службу спеціального зв'язку та захисту інформації України (ДССЗІ). Ця організація відповідає за координацію заходів з кібербезпеки, надання консультацій та підтримки, а також контролює впровадження заходів безпеки у критичних секторах (Малюта, Дерманська, 2019).

– Рівень кібератак та інцидентів

Україна стала однією з найбільш активних цілей кібератак в світі, особливо після початку конфлікту з росією в 2014 році. Рівень кіберзагроз в Україні значно зросла в останні роки, і це не тільки через військові конфлікти, але і через зростання кількості кіберзлочинів, які спрямовані на державні структури, бізнес та громадянське суспільство. У 2017 році Україна стала жертвою глобальної кібератаки, яка була спрямована на державні інфраструктури, бізнес та громадян. Ця атака спричинила низку проблем, зокрема відключення енергопостачання в ряді областей, а також порушення роботи деяких державних служб (Пантєлєєва, 2019).

За даними досліджень, більшість кібератак на Україну здійснюються з росії. Зокрема, українські експерти виявили кілька груп, які діють на замовлення російських спецслужб та виконують різні кібернапади на українські організації та інфраструктуру. Також, на території України працюють різні групи кіберзлочинців, які займаються шахрайством та вимагають викупи за шифрування даних (рансомвар). Кіберзагрози також є глобальною проблемою для критичної інфраструктури. Таким чином, в 2021 р. у США хакерське угрупування здійснило

кібератаку на найбільшу трубопровідну компанію і зупинило його роботу (Краснопольська, 2022).

Але, у 2022 році Україна посіла 24 місце в рейтингу Державного індексу кібербезпеки (National Cyber Security Index, 2022), який щорічно складає Фонд електронного урядування Естонії. Критерії, що впливають на оцінку включають спроможність держав ідентифікувати цифрові загрози, формувати механізми для їх запобігання і розвивати потрібні орієнтири в державі.

Відтак аналіз відповідності рівня цифрової безпеки в дипломатичних установах України є важливим інструментом для забезпечення безпеки інформації в державних органах. Підвищення рівня цифрової безпеки в дипломатичних установах є необхідною умовою для забезпечення національної безпеки та захисту національних інтересів України.

У 2023 році Україна офіційно стала членом Центру НАТО з питань співробітництва в галузі кіберзахисту (CCDCOE). Цей центр є акредитованим в НАТО хабом для кіберінформації, дослідницьким центром та організацією, що займається підготовкою та тренуванням фахівців з кібербезпеки. Військова організація зі штаб-квартирою в Таллінні фокусується на проведенні міждисциплінарних прикладних досліджень, консультаціях та підготовці фахівців у галузі кібербезпеки. Членство України в Центрі допоможе зміцнити обмін кібердосвідом з іншими країнами-учасницями. Україна має можливість поділитися своїм цінним досвідом з перших рядів щодо певних супротивників у сфері кібербезпеки, який можна використовувати для подальших досліджень, навчання та тренування (Українська правда, 2023).

2.2. Заходи з забезпечення цифрової безпеки дипломатичних установах України міжнародним стандартам та рекомендаціям

Держава ставить перед собою завдання постійного підвищення рівня цифрової безпеки в усіх державних органах, включаючи дипломатичні установи. Уряд України приділяє увагу розробці та виконанню програм дій забезпечення

цифрової безпеки, а також встановленню стандартів та процедур для запобігання кібератакам (Краснопольська, 2022).

Забезпечення цифрової безпеки в дипломатичних установах України базується на міжнародних стандартах та рекомендаціях, зокрема:

- У 2011 році було прийнято Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» та створено Державну службу спеціального зв'язку та захисту інформації України (ДСЗЗІ). ДСЗЗІ є центральним органом виконавчої влади, який забезпечує захист інформації в інформаційно-телекомунікаційних системах та здійснює державне регулювання у сфері захисту інформації (Піпченко, 2019).

– Конвенція про кіберзлочинність Ради Європи, яка визначає кіберзлочинність та надає рекомендації щодо захисту від кібератак.

Україна є стороною Конвенції про кіберзлочинність Ради Європи (далі – Конвенція), яка була підписана у Будапешті у 2001 році та ратифікована Україною у 2006 році. Конвенція є першим міжнародним документом, що визначає кіберзлочинність та встановлює правові засади для боротьби з нею. Конвенція передбачає визнання кіберзлочинів як злочинів, що підлягають кримінальному переслідуванню, а також визначає дії, які вважаються кіберзлочинами, такі як несанкціонований доступ до комп'ютерних систем, комп'ютерне шахрайство, порушення авторських прав у сфері комп'ютерних технологій, тероризм в Інтернеті, тощо (Краснопольська, 2022).

– Рекомендації НАТО з питань кібербезпеки, які стосуються захисту від кіберзагроз та розвитку кібероборони.

Однією з основних рекомендацій НАТО є забезпечення належного захисту критично важливих інфраструктур від кіберзагроз, зокрема, енергетичних, транспортних та інших систем. Крім того, рекомендації НАТО стосуються розвитку кібероборони та підвищення кваліфікації фахівців у галузі кібербезпеки. Україна активно впроваджує рекомендації НАТО та розвиває власну кібероборону, зокрема, створивши Кібербезпековий центр при Державній службі спеціального

зв’язку та захисту інформації та Національний координаційний центр кібербезпеки (НКЦК) (Краснопольська, 2022).

НКЦК є централізованою координаційною структурою, створеною з метою попередження, виявлення та ліквідації кібератак на державні інформаційні ресурси та критичну інфраструктуру України. Центр є державною організацією, яка допомагає взаємодії між державними органами, кампаніями та організаціями, що відповідають за питання цифрової безпеки. Завданням НКЦК є виявлення потенційних загроз кібербезпеці та координація заходів щодо їх запобігання та ліквідації. Центр також забезпечує підготовку кадрів у галузі кібербезпеки та розробку відповідних стандартів та нормативно-правових актів. У своїй діяльності НКЦК використовує сучасні методи та засоби захисту інформації, такі як системи виявлення вторгнень, інтелектуальний аналіз даних та інші технічні засоби. Крім того, центр здійснює постійний моніторинг кіберпростору, взаємодіє з міжнародними партнерами та координує взаємодію з відповідними структурами інших країн (Малюта, Дерманська, 2019).

– Рекомендації Європейського Союзу щодо кібербезпеки, які визначають рекомендації для захисту від кібератак та кіберзагроз.

4 березня 2021 робоча група при Національному координаційному центрі кібербезпеки Ради національної безпеки і оборони схвалила проєкт Стратегії кібербезпеки України на 2021–2025 роки. Президент України Володимир Зеленський прийняв рішення про введення в дію плану реалізації Стратегії кібербезпеки України, яке було схвалено Радою національної безпеки і оборони України. Відповідний указ президента був оприлюднений 1 лютого 2022 на офіційному сайті глави держави (Указ Президента, 2022).

Стратегія інформаційної безпеки України визначає принципи, спрямовані на захист національної безпеки в інформаційній сфері, протидію загрозам, захист прав осіб на інформацію та конфіденційності персональних даних. Головна особливість Стратегії полягає у тому, що вона встановлює загальні принципи інформаційної безпеки, незалежно від джерела загроз. У порівнянні з попередньою Доктриною 2017 року, яка реагує на застосування російською федерацією технологій гібридної

війни проти України, Стратегія пропонує переглянути інформаційне середовище без прив'язки до конкретної агресії з боку російської федерації. Багато з положень, викладених у Стратегії, залишатимуться актуальними й після закінчення війни з росією. Що стосується забезпечення цифрової безпеки в дипломатичних установах України необхідно зазначити, що заходів належать:

1. Розробка та впровадження політики забезпечення інформаційної безпеки, яка має включати процедури та стандарти з захисту інформації. Україна зобов’язалася виконувати рекомендації ЄС щодо кібербезпеки, які включають у себе ряд заходів, таких як: розробка та впровадження національної стратегії кібербезпеки та національної програми кіберзахисту; забезпечення безпеки критичної інфраструктури та інформаційних систем (Піпченко, 2019).

2. Забезпечення захисту персональних даних та інформації означає, що дипломатичні установи повинні розробити концепцію і стратегію забезпечення інформаційної безпеки, яка відповідала б міжнародним стандартам та рекомендаціям. Відповідно до цієї політики повинні бути визначені мета, завдання, основні принципи та підходи до забезпечення інформаційної безпеки в дипломатичних установах. Для цього можна використовувати рекомендації міжнародних стандартів, таких як ІСО/МЕК 27001 та ІСО/МЕК 27002, які регулюють системи управління інформаційною безпекою. Також, дипломатичні установи повинні розробити план дій з впровадження політики забезпечення інформаційної безпеки. В цьому сенсі мають бути визначені конкретні кроки, які потрібно зробити для забезпечення безпеки інформації в дипломатичних установах (Краснопольська, 2022).

3. Розвиток кадрового потенціалу з кібербезпеки – один зі способів розвитку кадрового потенціалу з кібербезпеки, також є засобом підвищення кваліфікації працівників дипломатичних установ через проведення спеціальних курсів та тренінгів з кібербезпеки. Це допоможе працівникам дипломатичних установ отримати необхідні знання та навички для захисту інформації від кібератак. Також можливим є вивчення кібербезпеки на рівні вищої освіти, наприклад, в рамках спеціальностей зі зв’язку, інформатики та інших суміжних напрямків. За такою

спеціальністю можуть навчатися студенти, які мають бажання працювати в дипломатичних установах та забезпечувати їхню цифрову безпеку (Малюта, Дерманська, 2019).

4. Забезпечення співпраці та обміну інформацією з іншими країн – Україна також має домовленості про співпрацю з іншими країнами з питань кібербезпеки. Наприклад, в 2018 році Україна підписала Меморандум про співпрацю в галузі кібербезпеки з США. У рамках цієї угоди Україна та США домовилися про співпрацю в області кібербезпеки, в тому числі про обмін інформацією та досвідом. Крім того, Україна є учасником різних міжнародних організацій, таких як Організація з безпеки і співробітництва в Європі (ОБСЄ), де також здійснюється співпраця в області кібербезпеки (Малюта, Дерманська, 2019).

5. Встановлення захисних засобів на комп'ютерах та мережевих пристроях, таких як антивірусні програми, фаєрволи та інші. Ці заходи допомагають запобігти вторгненням та іншим видам кібератак, що можуть привести до витоку конфіденційної інформації або порушення роботи комп'ютерних систем. Антивірусні програми дозволяють виявляти та вилучати зловмисний програмний код, в тому числі віруси, троянські програми та шпигунське програмне забезпечення. Фаєрволи ж контролюють доступ до мережі та блокують шкідливий трафік, що може бути викликаний кібератаками. Також фаєрвол може бути налаштований на блокування з'єднань з небезпечних IP-адрес або на фільтрацію трафіку на основі певних правил (Малюта, Дерманська, 2019).

6. Проведення навчання працівників дипломатичних установ щодо безпеки в IT та захисту від кібератак, яке має на меті забезпечити працівників дипломатичних установ необхідними знаннями та навичками, які дозволять їм бути впевненими у захисті своїх даних та інформації дипломатичної установи від кібератак. Основними завданнями навчання є надання працівникам дипломатичних установ навичок виявлення та попередження кібератак, забезпечення безпеки в роботі з електронною поштою та соціальними мережами, встановлення та налаштування антивірусних програм, робота з паролями та захистом своїх акаунтів, а також знання основ криптографії (Краснопольська, 2022). Навчання може проводитися як

в онлайн форматі, так і у формі тренінгів та семінарів зі спеціалістами з цифрової безпеки. Також, можливо провести навчання як внутрішньо в дипломатичній установі, так і залучити зовнішніх експертів з цифрової безпеки.

7. Оновлення систем захисту від кібератак та вірусів є також важливою складовою цифрової безпеки в дипломатичних установах. Оновлення систем захисту має на меті забезпечити захист від нових кіберзагроз та вірусів, які можуть виникнути в майбутньому. Оновлення може включати в себе встановлення оновлень програмного забезпечення, зміну налаштувань системи захисту та заміну застарілої антивірусної програми (Малюта, Дерманська, 2019).

8. Використання захисних технологій, таких як шифрування даних та підписування електронних документів – шифрування даних є ефективним заходом забезпечення безпеки цифрової інформації, оскільки воно дозволяє зашифрувати дані таким чином, щоб вони були незрозумілі для неповідомлених осіб. Застосування шифрування даних дозволяє забезпечити конфіденційність та цілісність інформації, що передається в електронному вигляді. Такі технології шифрування, як наприклад RSA або AES, є широко використовуваними в цьому контексті. Підписування електронних документів є іншим ефективним заходом забезпечення цифрової безпеки в дипломатичних установах. Підписання електронних документів забезпечує їх автентичність та незмінність, оскільки будь-яка зміна документу буде помічена як недійсна. Для підписування електронних документів використовуються криптографічні ключі та цифрові сертифікати, які забезпечують достовірність підпису. Ці заходи спрямовані на запобігання кіберзагрозам та кібератакам, захист даних, інформації та розумової власності дипломатичних установ України (Малюта, Дерманська, 2019).

Повинна бути також забезпечена належна фізична безпека дипломатичних установ, так як кіберзлочинці можуть використовувати техніки соціальної інженерії, щоб отримати доступ до важливих інформаційних ресурсів. Крім того, дипломатичні установи України повинні стежити за актуальними трендами та новими загрозами в галузі кібербезпеки, і відповідно оновлювати свої заходи забезпечення безпеки.

Висновки до розділу 2

1. У ході дослідження дипломатичних установ України було встановлено, що цифрова безпека є одним з найважливіших аспектів діяльності таких установ. Розвиток технологій і зростання загроз кібербезпеці вимагають постійного удосконалення заходів забезпечення безпеки в інформаційних системах дипломатичних установ. Для забезпечення цифрової безпеки в дипломатичних установах України необхідно застосовувати комплексний підхід, який включає в себе не лише застосування захисних технологій, але й навчання працівників, встановлення процедур реагування на кібератаки та кримінальні дії в ІТ, аудит та оновлення систем захисту від кібератак та вірусів.

2. Для підвищення рівня цифрової безпеки в дипломатичних установах України необхідно постійно вдосконалювати технічні та організаційні заходи забезпечення безпеки інформаційних систем, а також проводити регулярні навчання працівників у сфері кібербезпеки. Застосування такого комплексного підходу дозволить зменшити ризики кібератак та інших кіберзагроз і забезпечити надійний захист інформації в дипломатичних установах України.

3. Проте, з урахуванням постійного розвитку кіберзагроз та зростання рівня складності кібератак, необхідно постійно підвищувати рівень захисту інформації в дипломатичних установах. Тому важливим є постійний моніторинг та аналіз рівня цифрової безпеки в дипломатичних установах і проведення необхідних заходів з підвищення рівня захисту.

РОЗДІЛ 3
НАПРЯМКИ УДОСКОНАЛЕННЯ ЦИФРОВОЇ БЕЗПЕКИ В ДИПЛОМАТИЧНИХ УСТАНОВАХ УКРАЇНИ

3.1. Важливість забезпечення цифрової безпеки для дипломатії

Забезпечення цифрової безпеки в сучасному світі є критично важливим завданням для дипломатії. З урахуванням зростаючої кількості кібератак, віртуальних шпигунств та інших цифрових загроз, дипломатичні місії та організації повинні бути особливо уважними щодо збереження та захисту конфіденційної інформації. Втрата такої інформації може призвести до серйозних наслідків, включаючи порушення міжнародної безпеки, виток державних та комерційних таємниць, та навіть втручання в політичні процеси і вибори (Ляшенко, 2018).

Для цифрової дипломатії безпека перетворилася на багатогранний об’єкт, який вже не просто є «цифровою інформаційною безпекою», а саме «кібербезпекою», терміном, що поєднує і технічні, і соціальні, і політичні аспекти цього поняття. Вектори кібербезпеки інформаційних потоків містять як елементи, що легко розділяються за своєю природою, так і тісно пов’язані. Так, до технічної безпеки можна віднести поняття безпеки проведення транзакцій, конфіденційності відомостей, безпеки мереж, питання безпеки інфраструктурних об’єктів. При цьому безпека розуміється швидше як технічне питання: достовірність передачі даних з пункту А до пункту Б, безпека та адекватність програмного забезпечення тощо. При цьому про порушення безпеки рівнозначно можна говорити і в ситуації зловмисних дій 3-х осіб та у ситуації випадкових дій, помилок, аварій тощо (Der, 2011).

Якщо в 2010-х роках цифрова дипломатія полягала у лінійному поширенні інформації в соціальних мережах та була частиною публічної дипломатії, то в 2020-х роках дипломатія даних використовує алгоритми для фільтрації аудиторії, створення інформаційних кампаній та виявлення джерел недружньої інформації. У минулому фокус досліджень був спрямований на процес цифровізації

зовнішньополітичного механізму та залучення зарубіжної аудиторії, і загальна теза стверджувала, що цифрова дипломатія може бути ефективною в боротьбі з цифровими загрозами. У ті роки наукова думка була націлена на вивчення процесу цифрової трансформації зовнішньополітичного механізму, а також на розгляд питання щодо створення необхідної інформаційної стратегії та залучення до неї міжнародної аудиторії. Загальна теза досліджень заявляла, що цифрова дипломатія держав може бути ефективним інструментом для протидії цифровим акціям радикальних груп або груп опозиції (Малюта, Дерманська, 2019).

Ближче до 2015–2017 рр., з появою великої кількості акторів у соціальних мережах та інструментів для просування інформації, стратегії цифрової дипломатії стали спиратися на створення мереж впливових осіб (інфлюенсерів), які можуть впливати на своїх підписників. Це стало більш ефективним інструментом для просування позиції держави та боротьби з конкурентами, порівняно зі звичайним поширенням інформації. В зовнішній політиці почали використовувати алгоритми для фільтрації користувачів та цільового поширення інформації. З'явилися проекти, спрямовані на нейтралізацію пропаганди екстремістів та вплив на невеликі групи в Інтернеті (Bjola, Manor, 2018).

Проте, відбулася революція в розвитку цифрової дипломатії у період з 2018 по 2022 роки, коли сталася датафікація, що спричинила бурхливий і неконтрольований доступ до технологій штучного інтелекту, який дозволяє швидко впливати на цільову аудиторію за допомогою ефективних інформаційних кампаній, фільтрації, створення синтетичних ЗМІ та дип-фейків. Цифрові дипломати зрозуміли, що без використання аналізу великих обсягів даних неможливо створити ефективну цифрову інформаційну кампанію або вплинути на цільову аудиторію. Постійне зростання числа учасників, кібератаки, розширення інформаційних кампаній та твіттер-протести призвели до появи заплутаності (entanglement), про яку згадував Дж. Дер Деріан. (Der, 2011).

Концепцію квантової дипломатії (quantum diplomacy) Дер Деріана (2011) все частіше використовують для пояснення сучасного стану цифрових міжнародних відносин, де події, які здаються неспорідненими, переплітаються між реальністю і

цифровим відтворенням політики, а дипломатія повинна реагувати на всі інформаційні виклики в умовах невизначеності (Турчин, 2016). Цифрова невизначеність полягає в тому, що будь-яка інформація, що поширюється через соціальні мережі, може впливати на поведінку окремих соціальних груп та зовнішньополітичну діяльність держави. Офіційна дипломатія може бути підірвана більш ефективними інформаційними кампаніями недержавних акторів, таких як блогери, журналісти, кібердисиденти тощо (Ляшенко, 2018).

Цифрова трансформація розчленувала міжнародні відносини та створила мільйони конфліктуючих трактувань та інтерпретацій про те, що відбувається, як у словесному, так і візуальному форматі. Власники політичних реальностей та інформації в Інтернеті мають великий вплив на мільйони пасивних користувачів, що сприймають світову політику. У цьому фрагментованому цифровому світі цифрова дипломатія може формувати різні політичні реальності в соціальних мережах і стримувати інформаційні кампанії інших держав та неурядових акторів, просуваючи свій порядок денний, легітимізуючи власні дії та делегітимізуючи дії супротивників (Kassner, 2019).

Цифрова невизначеність та фрагментація вимагають проведення наступальної цифрової дипломатії. Спонсоровані державою платформи міжнародного мовлення або цифрової дипломатії працюють в умовах несподіваної та непередбачуваної конкуренції з блогерами, ЗМІ, які будь-якої миті можуть підірвати всі зусилля державної інформаційної машини. Лінійна дипломатія не працює, оскільки державні канали можуть програвати інформацію, яка йде від приватних блогерів чи ЗМІ (Малюта, Дерманська, 2019).

Виживання офіційної цифрової дипломатії в епоху датафікації залежить від розуміння практиками такого поняття, як фреймінг, що передбачає використання емоцій, тональності та різних практик для просування потрібного наративу або інформації. Офіційні канали держав здійснюють так зване кадрування подій у реальному часі для різних груп цільової аудиторії, щоб конкурувати з інформацією, що розповсюджується ЗМІ, журналістами та іншими акторами протилежної сторони (Турчин, 2016).

Розуміння цього процесу створює нову основу реалізації ефективної цифрової дипломатії. Вміле використання ключових слів та тональності постів сприяє просуванню масиву меседжів через масу розрізнених пабліків, луна камер, бульбашок фільтрів, які разом і становлять фрагментовану цифрову реальність (Ляшенко, 2018).

Очевидно, що лише аналітики даних здатні побудувати необхідні інформаційні кампанії або вивчити діяльність опонентів. Великі дані мають на увазі отримання набору даних та їх аналіз машинним способом. До малих даних відносяться обмежена кількість постів або твітів, отриманих із соціальних мереж ручним чи машинним способом (Kassner, 2019).

Довгий час вчені в галузі міжнародних відносин використовували малі дані, що було прийнятним для вивчення лінійної цифрової дипломатії. З метою запобігання цифрових загроз, дипломатичні місії розробляють та впроваджують стратегії цифрової безпеки, що включають у себе використання захищених систем зв'язку, шифрування конфіденційної інформації, та належну підготовку дипломатичного персоналу щодо цифрової безпеки та використання безпечних практик в Інтернеті. Крім того, дипломатичні місії повинні встановлювати зв'язки з місцевими експертами з цифрової безпеки, щоб отримувати поради та рекомендації щодо покращення безпеки своїх інформаційних систем (Малюта, Дерманська, 2019).

Однак, окрім технічних заходів, важливо забезпечити дотримання принципів академічної доброчесності та етики в дипломатичній діяльності. Це означає, що дипломати повинні дотримуватися правил збереження конфіденційної інформації та не використовувати інформацію від третіх сторін без згоди власників інформації. Дипломати повинні також дотримуватися принципу чесності і не вживати незаконних методів отримання інформації, що може призвести до негативних наслідків для міжнародних відносин (Ляшенко, 2018).

Окрім того, цифрова безпека є ключовим аспектом захисту державної та комерційної таємниці, обміну конфіденційною інформацією між державами та бізнес-структурами. Зловмисники можуть використовувати різноманітні методи

атак на цифрові системи, такі як шпигунство, крадіжка інтелектуальної власності, вимагання викупу зашифрованих даних, та інші (Турчин, 2016).

У сфері дипломатії також можуть бути спроби злому електронної пошти, соціальних мереж, месенджерів, мобільних пристроїв та інших електронних засобів зв'язку. Ці загрози можуть мати на меті отримання доступу до конфіденційної інформації, яка може бути використана для шантажу, спотворення інформації або навіть для відволікання уваги від важливих питань. Злом електронної пошти та інших засобів зв'язку може бути здійснений шляхом використання різних методів, таких як фішинг, віруси, шпигунський софт, внутрішні інсайдерські атаки тощо. В разі успішного злому, атакувач може отримати доступ до конфіденційної інформації, включаючи переписки, документи, звіти, контакти та іншу конфіденційну інформацію (Малюта, Дерманська, 2019).

Тому, для того щоб дипломатія могла ефективно працювати в умовах технологій, які швидко розвиваються, та загроз цифрової безпеки, необхідно забезпечити високий рівень захисту цифрових систем та інформації. Це можна зробити шляхом впровадження відповідних технічних заходів, які включають у себе захист мережі від кібератак, шифрування даних, двофакторну аутентифікацію, антивірусне програмне забезпечення та інші. Також необхідно підвищувати рівень обізнаності дипломатів щодо цифрової безпеки та проводити регулярні тренінги та семінари з цього питання (Карчева, Огородня, Опенько, 2017).

3.2. Пропозиції щодо удосконалення заходів забезпечення цифрової безпеки у дипломатії

Останнім часом дипломатичні організації України здійснюють активну діяльність у рамках цифрового простору, що є інструментом просування та поширення зовнішньополітичного курсу та зростання привабливості образу держави на міжнародній арені. Примітно, що суб'єктами глобального інформаційного середовища виступають не лише представники державної влади, а й транснаціональні корпорації, організації громадянського суспільства, спільноти

в соціальних мережах та фізичні особи. Таким чином, на публічну дипломатію в рамках цифрового простору впливають не лише органи державної влади, а й представники бізнесу та громадські організації (Малюта, Дерманська, 2019).

Одним із пріоритетних та перспективних напрямів підвищення ефективності забезпечення інформаційної безпеки у сфері публічної дипломатії є розробка заходів щодо активізації участі представників вітчизняних технологічних підприємств та підвищення популярності розробленого вітчизняними фахівцями програмного забезпечення та інтернет-платформ (Ляшенко, 2018).

Захист інформаційного поля дипломатичного відомства необхідний для забезпечення діяльності щодо добору достовірних, актуальних, вичерпних матеріалів та надання їх у вищі держоргани для прийняття правильних рішень на міжнародному рівні. Також це дає гарантію збереження секретної інформації, що зберігається в МЗС (Карчева, Огородня, Опенько, 2017).

Для вирішення цих завдань необхідно виконати такі заходи:

1. Впровадження строгих політик забезпечення кібербезпеки на всіх рівнях дипломатичної служби є важливим кроком для забезпечення безпеки інформаційних систем та захисту конфіденційної інформації в дипломатичних відносинах. Серед таких політик можуть бути вимоги до дипломатичних посадових осіб щодо використання захищених паролів, шифрування електронної пошти та інших форм зв’язку, використання безпечних мереж та програмного забезпечення, регулярна зміна паролів та перевірка на наявність вразливостей у програмному забезпеченні. Крім того, важливо проводити регулярну підготовку дипломатичного персоналу з питань кібербезпеки, включаючи навчання профілактичних заходів та дій в разі кібератак, вимог до поведінки в Інтернеті та безпечного використання пристроїв. На рівні керівництва дипломатичних місій також можуть встановлюватися вимоги до проведення регулярних аудитів безпеки інформаційних систем та належна підготовка з питань кібербезпеки та захисту від кібератак (Піпченко, 2015).

2. Попередження і виявлення цифрових загроз є важливим етапом забезпечення кібербезпеки дипломатії. Це означає виявлення можливих загроз, їх

аналіз та визначення ступеня важливості кожної з них. Один зі способів передбачення цифрових загроз – це використання інформаційно-аналітичних систем, які здатні відстежувати та аналізувати злочинну активність у кіберпросторі (Турчин, 2016). Ці системи допомагають виявляти потенційні загрози та інформувати дипломатичних працівників про їх наявність. Крім того, важливо вести систематичний моніторинг усіх діяльностей в мережі Інтернет, що стосуються дипломатичної діяльності, таких як згадки про дипломатів, їхні візити, зустрічі, а також усі інші активності, які можуть відобразити рівень інтересу інших держав до діяльності дипломатичної місії (Малюта, Дерманська, 2019).

Для розкриття цифрових загроз важливо розробляти механізми, які дозволяють виявляти, розслідувати та реагувати на кібератаки. Ці механізми повинні бути доступними на всіх рівнях дипломатичної служби та повинні включати у себе процедури збору доказів, проведення розслідувань, інформування та співпраці з іншими організаціями, які займаються кібербезпекою. Після виявлення потенційної кіберзагрози, необхідно визначити її ступінь важливості та відповідність до національних інтересів держави. Це допоможе зосередити зусилля на найбільш критичних аспектах захисту цифрових систем. Для розкриття загроз можна використовувати різні методики, такі як моніторинг систем, аналіз поведінки користувачів та технічний аналіз захисних систем. Однак, слід пам’ятати про важливість захисту персональних даних та конфіденційної інформації, тому в процесі виявлення та розкриття кіберзагроз необхідно дотримуватися відповідних етичних та правових норм (Bay, 2016).

Після розкриття та визначення ступеня важливості загрози, необхідно вжити заходів для забезпечення кібербезпеки. Це може включати в себе розробку та впровадження відповідних стратегій та політик забезпечення кібербезпеки, а також проведення навчань та підготовки персоналу щодо захисту цифрових систем. Також важливо забезпечувати постійний моніторинг та аналіз систем з метою виявлення нових загроз та швидкої реакції на них (Піпченко, 2015).

3. Визначення кола інформації, яка потребує охорони в цифровій дипломатії, є важливим етапом у забезпеченні кібербезпеки дипломатичних місій. Це коло

інформації може включати в себе конфіденційну інформацію про політичні переговори, зовнішньополітичні стратегії, розташування та захист дипломатичних місій, особисту інформацію дипломатів та інше. Охорона цієї інформації передбачає використання захищених систем зв'язку, шифрування конфіденційної інформації, та використання безпечних практик в Інтернеті. Важливо також встановлювати строгі політики доступу до цієї інформації, контролювати доступ до неї та проводити аудит безпеки систем зберігання цієї інформації (Піпченко, 2015).

Позначення кола інформації, яка потребує охорони, повинно бути здійснене відповідно до встановлених процедур та з урахуванням ступеня важливості цієї інформації для національної безпеки та інтересів держави. Для цього можуть використовуватись спеціальні класифікаційні системи, що дозволяють визначати ступінь важливості інформації та рівень її захисту. Наприклад, в США для цього використовується система класифікації інформації, що складається з чотирьох рівнів: «неприпустимої», «секретної», «доступної тільки з дозволу» та «несекретної» (Турчин, 2016).

4. Розробка та удосконалення правової бази є одним з ключових аспектів забезпечення цифрової безпеки у міжнародних взаємовідносинах. Національна та міжнародна законодавча база повинна бути достатньою, щоб забезпечувати захист інформації від потенційних кіберзагроз. Одним з основних елементів правової бази є розробка та впровадження національних та міжнародних законів, які регулюють використання кіберпростору в міжнародних відносинах та забезпечують захист країн від кіберзагроз. Для цього необхідно сприяти розробці міжнародних норм та стандартів, які регулюють поведінку держав у кіберпросторі та забезпечують захист від кібератак (Kassner, 2019).

Крім того, держави повинні розробляти свою власну національну стратегію цифрової безпеки, яка включатиме у себе не лише технічні заходи, але й політичні, економічні та правові аспекти. Національна стратегія повинна відображати основні цілі та завдання держави в галузі цифрової безпеки, а також передбачати заходи щодо взаємодії з міжнародними партнерами з метою забезпечення захисту від

кіберзагроз. Для вдосконалення правової бази забезпечення інформаційної безпеки у процесі міжнародних взаємовідносин необхідно також розробляти та удосконалювати механізми міжнародної співпраці в галузі цифрової безпеки. Важливим елементом правової бази є також розробка та впровадження стандартів безпеки для дипломатичної інформації, що допоможе забезпечити єдність підходів до захисту даних на різних рівнях дипломатичної служби та сприятиме підвищенню ефективності боротьби з цифровими загрозами (Bay, 2016).

5. Узгодження заходів щодо інформаційної захищеності між головним управлінням іноземного відомства та його підрозділами в інших державах в цифровій дипломатії є важливим елементом забезпечення кібербезпеки в дипломатичних відносинах. Це означає, що всі дипломатичні місії повинні дотримуватися єдиної політики забезпечення кібербезпеки, яка включає в себе розробку стратегій цифрової безпеки та використання захищених систем зв'язку та шифрування конфіденційної інформації (Малюта, Дерманська, 2019).

Узгодження таких заходів між головним управлінням іноземного відомства та його підрозділами в інших державах передбачає встановлення стандартів та процедур забезпечення кібербезпеки, які повинні дотримуватися всіма дипломатичними місіями. Це включає розробку інструкцій та планів дій для відповідного реагування на кібератаки, проведення тренувань та навчань дипломатичного персоналу з цифрової безпеки та використання безпечних практик в Інтернеті (Турчин, 2016).

Крім того, узгодження заходів щодо інформаційної захищеності між головним управлінням іноземного відомства та його підрозділами в інших державах передбачає встановлення системи контролю за кібербезпекою та звітності. Це може включати регулярні аудити та перевірки наявності потенційних ризиків безпеки, а також звіти про заходи, які були прийняті для забезпечення кібербезпеки. Для досягнення цієї мети можуть бути розроблені спільні протоколи забезпечення безпеки, стандарти зберігання та передачі інформації, а також засоби зв'язку, які гарантують безпеку та надійність передачі інформаці (Малюта, Дерманська, 2019).

Доцільним є створення спеціальних комітетів, які займатимуться координацією заходів з кібербезпеки між різними підрозділами дипломатичної служби. Такі комітети повинні включати представників різних державних органів, відповідальних за кібербезпеку, а також експертів з цієї галузі. Однак, необхідно враховувати, що різні країни можуть мати різні правові та культурні особливості, які можуть впливати на підходи до захисту інформації та застосування технологій кібербезпеки. Тому необхідно також розробити механізми для вирішення різних проблем, які можуть виникати в процесі узгодження заходів з кібербезпеки між різними країнами (Краснопольська, 2022).

6. Для забезпечення ефективної кібербезпеки національної інформаційної системи в цифровій дипломатії необхідна активна співпраця на міжнародному рівні. Для цього, держави повинні проводити регулярні наради і консультації з питань кібербезпеки на міжнародних форумах, таких як конференції, симпозіуми, робочі групи тощо. В рамках таких зустрічей представники держав можуть обмінюватися досвідом, надавати рекомендації та розвивати спільні стратегії з питань кібербезпеки. Додатково, необхідно проводити міжнародні перевірки та аудити інформаційних систем, щоб виявляти та ліквідовувати можливі вразливості та загрози. Такі перевірки можуть бути проведені за домовленістю міжнародних договорів та угод, а також у рамках співпраці між національними організаціями з кібербезпеки (Ляшенко, 2018).

Крім того, держави можуть співпрацювати з міжнародними організаціями з метою розробки та вдосконалення стандартів кібербезпеки. Такі організації, як Міжнародне агентство з атомної енергії (МАГАТЕ), Організація з безпеки та співпраці в Європі (ОБСЄ), та Європейський союз (ЄС) розробляють стандарти та рекомендації з питань кібербезпеки, які можуть бути використані для забезпечення безпеки національної інформаційної системи в цифровій дипломатії (Краснопольська, 2022).

Таким чином, активна діяльність на міжнародному рівні є важливим компонентом забезпечення кібербезпеки в дипломатії. Співпраця між країнами та міжнародними організаціями може допомогти у покращенні кібербезпеки та

захисту важливої інформації, що має стратегічне значення для національної безпеки (Ляшенко, 2018).

Проведення результативного нагляду є одним з ключових елементів забезпечення кібербезпеки в цифровій дипломатії. Цей процес має на меті постійний моніторинг і оцінку заходів забезпечення кібербезпеки, що вживаються дипломатичними службами на різних рівнях. У цифровій дипломатії результативний нагляд повинен здійснюватися на кількох рівнях. На першому рівні – це моніторинг і оцінка власної кібербезпеки держави. Кожна держава повинна проводити аналіз власної інформаційної системи з метою виявлення слабких місць і здійснювати заходи для їх усунення (Турчин, 2016).

На другому рівні результативний нагляд має на меті контроль за дотриманням встановлених правил і процедур забезпечення кібербезпеки дипломатичних служб. При цьому необхідно оцінювати ефективність заходів забезпечення кібербезпеки, виявляти проблемні аспекти та розробляти плани дій для подальшого покращення захисту. На третьому рівні – це моніторинг і оцінка кібербезпеки партнерських держав та їх дипломатичних служб. Цей рівень вимагає від держави тісного співробітництва з іншими країнами з метою обміну досвідом та інформацією про стан кібербезпеки. Окрім того, результативний нагляд повинен проводитися регулярно і бути орієнтованим на зміну загроз та ризиків в цифровій дипломатії. Це дозволить оперативно реагувати на нові види кібератак та вчасно вживати заходів щодо їх запобігання (Краснопольська, 2022).

Інтернет-краудсорсинг – ще один захід, що позитивно себе зарекомендував для просування публічної дипломатії, – є технологією координації зусиль різних членів суспільства в цифровому просторі. Вона дозволяє формувати інтерактивні карти загроз та ризиків для подальшого обговорення на всіх рівнях суспільства, створювати політико-дипломатичні спільноти на інтерактивній основі, а також своєчасно інформувати широкі верстви населення у разі настання кризових ситуацій.

Висновки до розділу 3

1. Розробка та прийняття цифрових ініціатив, з одного боку, може бути розглянута як серйозний виклик у сфері публічної дипломатії, оскільки цей процес радикально змінив розвиток дипломатичної діяльності, аспект управління та контролю інформації, проведення міжнародних переговорів та врегулювання криз.

2. Цифрова дипломатія має чимало переваг. Вона допомагає міжнародним суб'єктам, особливо державам, у досягненні цілей зовнішньої політики України. Сайти соціальних мереж, такі як Twitter та Facebook, розширили можливості спілкування, перетворивши його з монологу на діалог, дозволяючи урядовцям вести двосторонні бесіди з населенням. Ще однією перевагою є те, що соціальні мережі дозволяють дипломатам виглядати більш доступними та прозорими для громадськості, розвивають почуття суспільної довіри та зрештою дозволяють політикам розширити свій вплив. Цифрові технології надзвичайно корисні для збору та обробки інформації про дипломатичну діяльність, а також для швидкого зв'язку у невідкладних ситуаціях. Завдяки їм люди, які живуть за авторитарних режимів, можуть уникнути обмежень, що призводить до мінімізації авторитаризму. Цифрова дипломатія не завжди потребує фінансових вкладень та потребує менших витрат порівняно з іншими дипломатичними методами, що робить її привабливою для урядів, МЗС та посольств.

3. Однак, за всіх своїх переваг, цифрова дипломатія також розглядається як джерело загроз та ризиків. Анонімність, витік інформації, атаки хакерів можуть завдати шкоди як окремо взятим політичним фігурам, так і державам в цілому. Публікація недостовірної інформації, а також поширення особистої інформації користувачів, організацій, держав може призвести до складних міжнародних криз.

ВИСНОВКИ

Проведене дослідження яскраво проілюструвало, що у сучасному, все більш взаємопов'язаному світі, цифрова безпека стала першочерговою проблемою для урядів і дипломатичних установ у всьому світі. Дослідники дедалі більше фокусуються саме на питаннях цифрових загроз при здійсненні дипломатичної діяльності. Швидкий розвиток технологій надав сфері дипломатії як широкі можливості, так і серйозні виклики. Із зростанням залежності від цифрових систем і комунікаційних мереж зростає потреба в надійних заходах для захисту конфіденційної інформації та захисту дипломатичних інтересів.

В результаті цього дослідження було досягнуто поставленої мети та вирішено поставлені завдання. За підсумками дослідження можна зробити наступні висновки:

1. Визначено, що цифрову дипломатію можна охарактеризувати, як напрямок публічної дипломатії метою якого є просування політичних інтересів держави за кордоном, зміцнення іміджу держави на міжнародній арені, а також вибудовування зв'язків з урядовими структурами та громадянським населенням зарубіжних держав. Цифрова безпека має значення для дипломатії, оскільки сучасна дипломатична діяльність передбачає активне використання цифрових технологій для просування політичних інтересів держави за кордоном, зміцнення іміджу держави на міжнародній арені, а також вибудовування зв'язків з урядовими структурами та громадянським населенням зарубіжних держав. Зі збільшенням доступу до інформації та розвитком нових технологій збільшується нестабільність та слабкість контролю, що має наслідки для національної безпеки та міжнародних взаємин.

2. З'ясовано, що дипломатія у сфері цифрової безпеки стикається з ризиками та загрозами, що можуть мати серйозні наслідки для державної безпеки та взаємовідносин між країнами: кібератаки, дезінформація та фейки, шпигунство, залежність від технологій, використання інформації та соц-платформ для

поширення тероризму та екстремізму, швидке застаріння знань та компетенцій; низька комунікаційна культура у соц. мережах, що призводить до образ та конфліктів; передчасне розповсюдження та розсекречення даних; поширення фейкової та конфліктної інформації; постійний ризик хакерських атак та взлому інформаційних ресурсів; інвестиції в цифрову безпеку можуть спричинити гонку кіберозброєння; міжнародні норми з кібербезпеки не мають юридичної обов'язковості, складність у реалізації ефективних методів контролю політики цифрової безпеки; відсутність достатнього рівня консолідації міжнародних акторів для встановлення спільних норм з огляду на різне бачення поняття «свобода» у цифровому просторі; оскільки у інформаційному середовищі діючим об'єктом є індивід, інформація може викликати непередбачувані хвильові ефекти на внутрішньому і зовнішньому рівнях держави; національна політика все ще реагує на загрози як постійну умову, а не передбачає на керує станом.

3. Виокремлено, що сучасний досвід та практики забезпечення цифрової безпеки в дипломатії включають ряд заходів, спрямованих на попередження кібератак та захист інформації: підтримка країнами рекомендацій, що надають описані у роботі організації та конвенції; поширення провідними країнами досвіду та знань, проведення навчання в інших країнах; використання фільтрації аудиторії та поширення інформації, шифрування, електронних підписів, фреймінгу, позначеного кола інформації, захищених систем зв'язку та ін.

4. Систематизовано такі заходи з забезпечення цифрової безпеки дипломатичних установ України міжнародним стандартам та рекомендаціям: на основі міжнародних стандартів дипломатичні установи України підтримують Конвенцію про кіберзлочинність Ради Європи, стандарти ІСО/МЕК 27001 та ІСО/МЕК 27002, Рекомендації НАТО з питань кібербезпеки, Рекомендації Європейського Союзу щодо кібербезпеки; створюють та впроваджують структури для попередження та захисту від кібератак на державні інформаційні ресурси та критичну інфраструктуру; ведуть співпрацю та обмін інформацією з іншими країнами та організаціями; встановлюють захисні засоби на пристроях; використовують

технології шифрування даних, криптографічних методів, електронних підписів, оновлення систем захисту та програмного забезпечення; схвалено проєкт Стратегії кібербезпеки України на 2021–2025 рр.; приєднання України до акредитованого в НАТО хабу інформації CCDCOE., оскільки технології стали необхідною складовою міжнародних відносин.

5. Забезпечення цифрової безпеки важливо для дипломатії з огляду на поширене використання цифрових технології у здійсненні дипломатичної діяльності для оперативного зв'язку, збору і обробки інформації та зростаючу кількість кібератак, шпигунств, неправдивої інформації та загроз. Проаналізовані ризики та загрози свідчать про те що інформація є стратегічним ресурсом держави, і її втрата для представників дипломатичних організацій, відсутність знань щодо використання цифрових технологій, Інтернету та соціальних медіа може призвести до серйозних наслідків у порушенні міжнародної та національної безпеки, витоку таємниць, маніпулюванням даних та втручання у різні політичні процеси. Забезпечення цифрової безпеки також важливо для забезпечення довіри від зарубіжних партнерів. Якщо державна інформація підлягає крадіжці та витоку, це може спричинити складнощі у відносинах з іншими державами та міжнародними організаціями. Така нестабільність у поєднанні з різними (не)прийнятими нормами серед акторів та зростанням нових технологічних можливостей робить цифрову безпеку одним з центральних факторів у формуванні стратегій національних політик та політик відповідних структур щодо забезпечення безпеки їх дипломатичної діяльності.

6. Надані основні пропозиції щодо вдосконалення заходів забезпечення цифрової безпеки в дипломатії, які можуть включати наступне: розробка і впровадження стратегічних планів забезпечення цифрової безпеки, які враховуватимуть специфіку роботи дипломатичних установ та їхню залежність від інформаційних технологій; підвищення рівня свідомості та навичок з цифрової безпеки серед дипломатичного персоналу, включаючи проведення регулярних тренінгів та навчань; впровадження сучасних технологій захисту інформації, таких як

шифрування даних, двофакторна автентифікація та системи виявлення вторгнень; розробка та впровадження політики заборони використання особистих пристроїв у роботі з конфіденційною інформацією та встановлення механізмів контролю за виконанням цієї політики; підвищення рівня співпраці з іншими державами та міжнародними організаціями з метою обміну досвідом та інформацією щодо захисту інформації; підвищення рівня координації між різними дипломатичними установами та міністерствами в Україні, що забезпечить ефективнішу роботу та захист інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Європейська дипломатія у XXI столітті: матеріали IV науково-практичного круглого столу*. (2021). за ред. Л. В. Новікової, О. М. Доценко. Х. : ХНУ імені В. Н. Каразіна.
2. Карчева, Г., Огородня, Д., Опенько, В. (2017). Цифрова економіка та її вплив на розвиток національної та міжнародної економіки. *Фінансовий простір.* №3 (27). 10-23
3. Краснопольська, Т. (2022). Цифрова дипломатія як основа нової публічної дипломатії. *Актуальні проблеми політики: зб. наук. пр. редкол.* НУ «ОЮА», Південноукр. центр гендер. проблем. Одеса: Видавничий дім «Гельветика».
4. Ляшенко, В. (2018). *Цифрова модернізація економіки України як можливість проривного розвитку*: монографія; НАН України, Ін-т економіки пром-сті.
5. Малюта, Л., Дерманська, Л. (2019). Інноваційно-цифрові перспективи розвитку економіки України. Вчені записки Таврійського національного університету імені В. І. Вернадського. *Економіка і управління*. № 2. 55-60.
6. Макаренко, Є., Рижков, М. (2019). *Цифрова дипломатія*. Київ. нац. ун-т ім. Тараса Шевченка. Київ : ВАДЕКС.
7. Максименко, С., Кіш, Є., Лендьєл, М., Студенніков, І. (2015). *Регіональна політика в країнах Європи*: Уроки для України. Київ : Логос.
8. Про основні засади забезпечення кібербезпеки України. Закон України від 5 жовтня 2017 року. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
9. Піпченко, Н. (2015). *Міжнародна інтернет-комунікація як інструмент зовнішньополітичної діяльності*: автореф. дис. ... д-ра політ. наук : 23.00.04; Київ. нац. ун-т ім. Тараса Шевченка. Київ.
10. Піпченко, Н. (2014). *Соціальні медіа у структурі зовнішньої політики провідних міжнародних акторів.* Київ : Центр вільної преси.
11. Піпченко, Н. (2019). *Цифрова дипломатія.* Київ. нац. ун-т ім. Тараса Шевченка. Київ : ВАДЕКС.

12. *Політика культурної дипломатії: стратегічні пріоритети для України.* (2016). зб. наук.сперт. Матеріалів. Нац. ін-т стратег. дослідж.; упоряд. О. П. Розумна ; за заг. ред. О. П. Розумної, Т. В. Черненко. Київ : НІСД.
13. Пантєлєєва, Н. (2019). *Цифрова економіка як ключовий тренд розвитку постіндустріального суспільства*: монографія. Київ. ДВНЗ «Університет банківської справи».
14. Пантєлєєва, Н. (2020). Фінансова безпека в умовах цифрової економіки: очікування і реальність. *Фінансовий простір.* №2 (38). 22-37.
15. Піпченко, Н. (2015). Цифрова дипломатія як інструмент зовнішньополітичної діяльності США. *Міжнародні відносини. Серія «Політичні науки».* № 5. 15-26.
16. Турчин, Я. (2016). Інституційні правові основи е-дипломатії США. *Інформація, комунікація, суспільство*. №10. 15-25
17. Турчин, Я. (2013). Теорія і практика е-дипломатії у сучасних міжнародних відносинах. *Гілея: науковий вісник: зб. наук. пр. К.: Вид-во НПУ ім. М.П. Драгоманова,* № 7. 373-376.
18. Указ Президента України від 25 лютого 2017 р. № 47 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». https://zakon.rada.gov.ua/laws/show/47/2017#Text
19. Указ Президента України від 14 вересня 2020 р. № 392 «Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року «Про Стратегію національної безпеки України». https://zakon.rada.gov.ua/laws/show/392/2020#Text
20. Стратегія публічної дипломатії Міністерства закордонних справ України 2021-2025. https://mfa.gov.ua/storage/app/sites/1/%D0%A1%D1%82%D1%80%D0%B0%D1%82%D0%B5%D0%B3%D1%96%D1
21. Указ президента України №37/2022 «Про рішення Ради національної безпеки і оборони України від 30 грудня 2021 року «Про План реалізації Стратегії

кібербезпеки України» Retrieved from: https://www.president.gov.ua/documents/372022-41289

22. Україна офіційно вступила до кіберцентру при НАТО. "ЄВРОПЕЙСЬКА ПРАВДА" — ВІВТОРОК, 16 ТРАВНЯ 2023. https://www.pravda.com.ua/news/2023/05/16/7402456/
23. Україна офіційно вступила до кіберцентру при НАТО. Європейська правда. 16 травня 2023. Retrieved from: https://www.pravda.com.ua/news/2023/05/16/7402456/
24. Bjola, C., Manor I. (2018). Revisiting Putnam's two-level game theory in the digital age: domestic digital diplomacy and the Iran nuclear deal. Published online: 06 Jun 2018. Retrieved from: https://www.tandfonline.com/doi/abs/10.1080/09557571.2018.1476836
25. Bay, M. (2016). What is cybersecurity? French Journal for Media Research. Retrieved from: http://frenchjournalformediaresearch.com/index.php?id=988
26. Boulton, C. (2016). Whaling emerges as major cybersecurity threat. CIO. Retrieved from: http://www.cio.com/article/3059621/security/whaling-emerges-as-majorcybersecurity-threat.html
27. Cyber Security Strategy for Germany. Retrieved from: https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html
28. Der, D. (2011). Quantum Diplomacy, German-US Relations and the Psychogeography of Berlin, The Hague Journal of Diplomacy, vol. 6, no. 3–4, pp. 373–392
29. Farrell, S. (2016). Big hack attack: Protecting corporate reputation and brand value in the wake of a data breach. The Public Relations Strategist. Retrieved from: http://www.prsa.org/Intelligence/TheStrategist/Articles/view/11571/1129/Big_Hack_Attack_Protecting_Corporate_Reputation_an#.WHuGS4WcGJM
30. Field, T. (2016). Ransomware response study. Retrieved from: http://f6ce14d4647f05e937f4-

4d6abce208e5e17c2085b466b98c2083.r3.cf1.rackcdn.com/2016-ransomwareresponse-study-pdf-3-w-2983.pdf

31. Graham, S. (2020). Online Harms and the Legality Principle. Retrieved from :https://www.cyberleagle.com/2020/06/online- harms-and-legality-principle.html
32. International Organization for Standardization & International Electrotechnical Commission, Joint Technical Committee ISO/IEC JTC. Information technology – Security techniques – Guidelines for cybersecurity. Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en
33. Kassner, M. (2019). Anatomy of the Target data breach: Missed opportunities and lessons learned. ZDNet. Retrieved from http://www.zdnet.com/article/anatomy-of-thetarget-data-breach-missed-opportunities-and-lessons-learned/KPMG
34. Kasper, A., Vernigora, V. (2021) The EU's cybersecurity: a strategic narrative of a cyber power or a confusing policy for a local common market? *Journal of European Studies*, #65, 29-71. Retrieved from: https://doi.org/10.18543/ced- 65-2021pp29-71
35. Kurbalija, J., Hone, K. (2021). The Emergence of Digital Foreign Policy. Retrieved from: https://www.diplomacy.edu/sites/default/files/2021-03/2021_The_emergence_of_digital_for-eign_policy.pdf
36. Kalathil, S. (2013). *Diplomacy, Development, and Security in the Information Age.* Washington: Institute for the Study of Diplomacy, Georgetown University. Retrieved from: https://onlinebooks.library.upenn.edu/webbin/book/lookupid?key=olbp64936
37. Lord, N. (2016). What is a phishing attack? Defining and identifying different types of phishing attacks. Digital Guardian. Retrieved from: https://digitalguardian.com/blog/what-phishing-attack-defining-and-identifying-differenttypes-phishing-attacks
38. Michael N. Schmitt (Ed.) (2013). *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations.* National Security Archive. https://nsarchive.gwu.edu/news/cyber-vault/2019-04-24/tallinn-manual-20-international-law-applicable-cyber-operations

39. National Cyber Security Index. Retrieved from: https://ncsi.ega.ee/ncsi-index/
40. National Institute of Standards and Technology, USA. Retrieved from: https://www.nist.gov/
41. Pamment, J. (2016). *British Public Diplomacy and Soft Power: Diplomatic Influence and the Digital Revolution*. Palgrave MacMillan. Basingstoke: Palgrave Macmillan
42. Putnam, R. (1988). Diplomacy and Domestic Politics: The Logic of Two-Level Games. *International Organizations*, #3. 427-460.
43. Psaila, S. (2021). Improving the practice of cyber diplomacy: trainings, tools, and other resources. Retrieved from: https://www.diplomacy.edu/wp-content/uploads/2021/10/Cyber-diplomacy-study-Diplo-Phase-I.pdf
44. Public Diplomacy: Strengthening U.S. Engagement with the World. USC Center on Public Diplomacy. Retrieved from: https://uscpublicdiplomacy.org/sites/uscpublicdiplomacy.org/files/legacy/pdfs/PD_US_World_Engagement.pdf
45. Renard, T. (2018). EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*, #19 (3), 1-18.
46. Riordan, S. (2016). *Cyber Diplomacy vs Digital Diplomacy*: A Terminological Distinction. Retrieved from: https://uscpublicdiplomacy.org/blog/cyber-diplomacy-vs-digi-tal-diplomacy-terminological-distinction
47. Ruffini, B. (2017). *Science and Diplomacy: A New Dimension of International Relations.* Springer International Publishing.
48. Schwarzenbach, B.(2015). *Twitter and diplomacy:* How social media revolutionizes interaction with foreign policy. Retrieved from: http://thediplomaticenvoy.com/2015/10/12/twitter-and-diplomacy-how-social-media-revolutionizesour-interaction-with-foreign-policy/
49. Solomon, R. (2000). *The internet and the diffusion of diplomacy, US foreign policy Agenda*. Retrieved from: www.usinfo.state.gov/journals/itps

50. Sotiriu, S. (2015). Digital diplomacy: Between promises and reality. In C. Bjola & M. Holmes (Eds.), Digital diplomacy: Theory and practice. New York, NY: Routledge.
51. The US has announced its National Cybersecurity Strategy: Here's what you need to know. Retrieved from: https://www.weforum.org/agenda/2023/03/us-national-cybersecurity-strategy/
52. Westcott, N. (2008). Digital Diplomacy: The Impact of the Internet on International Relations. *Oxford Internet Institute, Research Report.*

АНОТАЦІЯ

Кваліфікаційної роботи

Тема: «Проблеми цифрової безпеки та її значення для дипломатії: аналіз загроз та ризиків»

Студент: Сабашенко Марія Сергіївна

Рік навчання, факультет: 4 р.н., ФСНСТ

Науковий керівник: Гош Мрідула, Доктор філософії, старший викладач

Рецензент:

Захищена “____”_____20_ р.

Короткий зміст роботи:

Ця робота концентрується на перетині цифрової безпеки та цифрової дипломатії, досліджуючи виклики, загрози та ризики, з якими стикається сучасний цифровий ландшафт. У роботі розглядаються теоретичні аспекти цифрової безпеки, пояснюється її концепція та значення для дипломатії, а також практичні особливості цифрової безпеки в дипломатичних установах України та сучасний досвід з забезпечення кібербезпеки інших країн. Пропонуються рекомендації щодо посилення заходів цифрової безпеки в українських дипломатичних установах відповідно до міжнародних стандартів і рекомендацій. Ця робота має на меті забезпечити розуміння дифузного середовища міжнародних відносин в епоху цифровізації, а представлені рекомендації можуть сприяти подальшому дискурсу про цифрову безпеку у дипломатії та створенню більш захищеного простору для дипломатичної діяльності.

Ключові слова: цифрова безпека, кібербезпека, цифрова дипломатія, інформаційна безпека, кібератаки

Short summary:

The thesis focuses on the intersection of digital security and digital diplomacy; exploring the challenges and threats facing today's digital landscape. The work examines theoretical aspects of digital security, explains its concept and significance for diplomacy, as well as practical features of digital security in diplomatic institutions of Ukraine and modern experience in ensuring cyber security of other countries. Recommendations are offered to strengthen digital security measures in Ukrainian diplomatic institutions in accordance with international standards and recommendations. This work aims to provide an understanding of the diffuse environment of international relations in the era of digitalization, and the presented recommendations can contribute to the further discourse on digital security in diplomacy and the creation of a more secure space for diplomatic activity.

Key words: digital security, cyber security, digital diplomacy, information security, cyber attacks