МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет права, публічного управління
та національної безпеки
Кафедра економічної теорії,
інтелектуальної власності та публічного
управління

Кваліфікаційна робота
на правах рукопису

СОРОКОПУД ВІКТОР АНАТОЛІЙОВИЧ
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК: 351.82
(індекс)

КВАЛІФІКАЦІЙНА РОБОТА

МІЖНАРОДНА СПІВПРАЦЯ УКРАЇНИ У СФЕРІ КІБЕРБЕЗПЕКИ: ВИКЛИКИ ТА СТРАТЕГІЇ
(тема роботи)

281 «Публічне управління та адміністрування»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр
кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

В. А. СОРОКОПУД
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи:
ВОЙТЕНКО Архип Борисович
(прізвище, ім'я, по батькові)

кандидат наук з державного управління, професор
(науковий ступінь, вчене звання)

Житомир – 2024

Висновок кафедри економічної теорії, інтелектуальної власності та публічного управління за результатами попереднього захисту: **СОРОКОПУДА Віктора Анатолійовича** допущено до захисту.

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № ____ від «____» грудня 2024 р.

Завідувач кафедри економічної теорії, інтелектуальної власності та публічного управління
к.е.н., професор _____ Валентина ЯКОБЧУК
(науковий ступінь, вчене звання) (підпис) (власне ім'я та прізвище)

«___» _____ 2024 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої **СОРОКОПУД Віктор Анатолійович** захистив
(прізвище ,ім'я, по батькові)

кваліфікаційну роботу з оцінкою:
сума балів за 100-бальною шкалою _____
за національною шкалою _____

Секретар ЕК
_____ _____ Анастасія ПРУТ
(науковий ступінь, вчене звання) (підпис) (власне ім'я та прізвище)

АНОТАЦІЯ

СОРОКОПУД В. А. Міжнародна співпраця України у сфері кібербезпеки: виклики та стратегії. – Кваліфікаційна робота на правах рукопису. Кваліфікаційна робота на здобуття освітнього ступеня магістра за спеціальністю 281 – Публічне управління та адміністрування. – Поліський національний університет, Житомир, 2024.

У кваліфікаційній роботі розглядається міжнародна співпраця України у сфері кібербезпеки, що є актуальною темою в умовах глобалізації та зростання загроз у кіберпросторі. Акцент зроблено на основних викликах, з якими стикається Україна, зокрема кібератаки з боку державних і недержавних суб'єктів, технологічна залежність, а також потреба у вдосконаленні національної інфраструктури безпеки. Проаналізовано основні напрями міжнародної взаємодії, зокрема співпрацю з НАТО, Європейським Союзом та стратегічними партнерами у сфері обміну досвідом, розробки спільних стратегій реагування на кіберзагрози та впровадження новітніх технологій. Запропоновано стратегії посилення міжнародного співробітництва, що включають інтеграцію до глобальних ініціатив у кібербезпеці, розбудову публічно-приватного партнерства та розвиток кібердипломатії. Особливу увагу приділено ролі України як одного з ключових гравців у забезпеченні регіональної стабільності у кіберпросторі.

Ключові слова: безпека, національні інтереси, виклики, кібербезпека,, міжнародна співпраця, стратегія.

SUMMARY

SOROKOPUD V. International cooperation of Ukraine in the field of cybersecurity: challenges and strategies. – Qualification work on the rights of the manuscript. Qualification work for obtaining a master's degree in specialty 281 «Public management and administration» – Polissia National University, Zhytomyr, 2024.

The qualification work examines Ukraine's international cooperation in the field of cybersecurity, which is a relevant topic in the context of globalization and growing threats in cyberspace. The emphasis is on the main challenges faced by Ukraine, including cyberattacks by state and non-state actors, technological dependence, and the need to improve the national security infrastructure.

The main areas of international cooperation are analyzed, in particular, cooperation with NATO, the European Union and strategic partners in the field of experience exchange, development of joint strategies for responding to cyber threats and introduction of the latest technologies. The author proposes strategies for strengthening international cooperation, including integration into global cybersecurity initiatives, building public-private partnerships, and developing cyber diplomacy. Particular attention is paid to the role of Ukraine as a key player in ensuring regional stability in cyberspace.

Keywords: security, national interests, challenges, cybersecurity, international cooperation, strategy.

ЗМІСТ

ВСТУП

Актуальність дослідження. Міжнародна співпраця України у сфері інформаційної безпеки є надзвичайно актуальною з огляду на сучасні глобальні загрози у кіберпросторі, що вимагає об'єднання зусиль країн для протидії викликам. Україна є одним із основних об'єктів кібератак у світі, особливо з боку державних агресорів, вже з 2014 року спостерігається системне втручання у критичну інфраструктуру країни, ідуть атаки на енергетичний сектор, кібератаки на держустанови, проводяться дезінформаційні кампанії та кібершпигунство. Ці загрози змушують Україну посилювати міжнародну кооперацію з іншими державами та організаціями для обміну досвідом і технологіями.

Кіберзагрози є важливою складовою сучасних гібридних воєн, а у випадку України ці загрози є частиною конфлікту з російською федерацією, чому сприяє відсутність чітких міжнародних норм у сфері кібербезпеки, що ускладнює відповідь на ці виклики та вимагає посиленої дипломатичної співпраці. Україна активно розвиває співробітництво з НАТО по Програмі посилення кіберзахисту та надання технічної допомоги Україні з ЄС, бере участь в ініціативах EU Cybersecurity Strategy, з США та іншими державами.

Наша держава бере участь в цифрових альянсах з IT-гігантами, такими як Microsoft, Google для покращення кіберзахисту. Ця співпраця забезпечує Україні доступ до передових технологій, аналітики, а також спільної протидії загрозам. При організації співпраці в сфері кібербезпеки в Україні виникають проблеми недостатньої координації міжнародних зусиль, обмеженість ресурсів для впровадження сучасних кіберрішень, юридичний вакуум в питаннях міжнародного кіберправа, низький рівень кіберграмотності в окремих державних структурах.

Україна може підвищити ефективність міжнародної взаємодії через активізацію участі у глобальних кіберініціативах, шляхом залучення інвестицій у кіберзахист через міжнародні програми, через інтеграцію до кіберстратегій

НАТО та ЄС, розвиток державно-приватного партнерства у сфері кібербезпеки та посилення кадрової підготовки фахівців у сфері кіберзахисту за підтримки міжнародних партнерів.

Відомими науковцями, які розробили підходи, оцінки значення міжнародного співробітництва у сфері кібербезпеки були Вудро Вільсон, Генрі Кісенджер, Роберт Кеохейн, Лестер Пірсон, кібербезпеки розглядали українські науковці Василенко, М. В. Гармаш О.П. та інші вчені.

Метою кваліфікаційної роботи є розкрити шляхи посилення міжнародної співпраці України в сфері кібербезпеки через та розробити рекомендації по побудові міжнародної стратегії . Сформована мета роботи дозволила *поставити ряд завдань:*

- розкрити етапи еволюції теорій міжнародного співробітництва в сфері кібербезпеки;

- показати особливості сучасної міжнародної політики в контексті нових викликів та кіберзагроз;

- проаналізувати інструменти впливу міжнародного співробітництва на кібербезпековий простір;

- розкрити загрози в сфері кібербезпеки на глобальному рівні;

- показати стратегічні напрями побудови політики боротьби з кіберзагрозами на міжнародному рівні.

Об'єктом дослідження є процес організації міжнародної співпраці в сфері кібербезпеки.

Предметом дослідження є актуальні проблеми підвищення ефективності міжнародної співпраці України у контексті посилення кіберзагроз.

У досягненні мети кваліфікаційної роботи використовувались загальні і спеціальні *методи,* системни аналіз, порівняння, монографічний підхід, елементи моделювання.

Перелік публікацій за темою дослідження. Результати досліджень доповідались на Міжнародних науково-практичних конференціях, за підсумками роботи опубліковано три публікації.

Практичні результати дослідження полягають в тому, що їх можна використовувати при формуванні міжнародної стратегії кібербезпеки.

До елементів наукової новизни роботи належить спроба автора визначити шляхи розвитку міжнародної співпраці України в сфері кібербезпеки.

Інформаційною базою дослідження стали наукові праці вітчизняних і зарубіжних вчених, статистичні збірники, нормативно-правова база, мережа Інтернет.

Кваліфікаційна робота містить вступ, три розділи та висновки до них, загальні висновки, список використаних джерел та додатки. Основний текст роботи викладено на 42 сторінках. Список використаних джерел включає 40 найменувань.

РОЗДІЛ 1.
ТЕОРЕТИЧНІ ЗАСАДИ ОРГАНІЗАЦІЇ МІЖНАРОДНОЇ СПІВПРАЦІ В СФЕРІ КІБЕРБЕЗПЕКИ

1.1. Суть та теорії організації міжнародної співпраці в сфері кібербезпеки

Міжнародна співпраця України у сфері кібербезпеки є важливим структурним елементом забезпечення національної безпеки, враховуючи інтенсивність сучасних загроз, глобальну координацію дій, обмін інформацією та інноваційними рішеннями, що є критично важливими для захисту держави у цифровій епосі. Теоретичні засади організації міжнародної співпраці в сфері кібербезпеки базуються на взаємодії держав, міжнародних організацій, приватного сектору та інших суб'єктів у рамках загальновизнаних принципів, концепцій та міжнародно-правових норм. Ці засади забезпечують основи для координації, регулювання та спільної протидії глобальним кіберзагрозам.

Теоретико-методологічні основи осмислення міжнародної співпраці в сфері кібербезпеки ґрунтуються на розумінні базових понять, а саме, категорії кіберпростір, як глобального інтегрованого середовища, яке включає інформаційну інфраструктуру та комунікаційні технології. Базовим поняттям є кіберзагроза – потенційна або реальна дія, що може завдати шкоди інформаційним системам або порушити їх функціонування, кібербезпека, як система заходів, спрямованих на забезпечення цілісності, доступності та конфіденційності інформації в кіберпросторі та міжнародна співпраця, це спільна діяльність держав та інших суб'єктів для досягнення глобальної безпеки у кіберсередовищі [1].

Протягом тривалого періоду часу формувались теоретичні концепції міжнародної співпраці у сфері кібербезпеки, насамперед це концепція колективної безпеки, вона передбачає, що загрози кібербезпеці однієї держави автоматично є загрозами для інших держав, прикладом є політика НАТО, що

застосовує принцип колективного захисту у кіберсфері, де атака на одну країну-члена розглядається як атака на весь альянс. Концепція колективної безпеки є однією з основ розвитку міжнародних відносин, яка стосується забезпечення спільної безпеки групи держав, колективного реагування на виклики. Мета побудови концепції запобігти агресії шляхом спільного реагування міжнародної спільноти за принципом «Атака на одного – це атака на всіх», через введення спільних санкцій, за допомогою дипломатичного тиску, військових або кібернетичних контрзаходів.

Провідною ідеєю колективної безпеки є створення державами організації або коаліції для спільного захисту від загроз, що виникають як у традиційній сфері (військові конфлікти), так і у нових сферах (кібербезпека, тероризм, екологічні катастрофи). Концепція колективної безпеки, також походить з ідей ліберального інтернаціоналізму, що акцентує увагу на можливості міжнародного співробітництва та створенні стабільного світу через спільні дії на основі засад**:**

1. Визнання спільних загроз, тобто агресія проти однієї держави загрожує безпеці всього міжнародного співтовариства.

2. Інституціоналізація безпеки, визначається тим, що міжнародні організації відіграють ключову роль у координації колективних дій.

3. Баланс сили і кооперація, які створюють стримуючий ефект, адже агресор ризикує зіткнутися з об’єднаною відповіддю інших держав [2].

Найвідомішими представниками концепції колективної безпеки були Вудро Вільсон, Президент США, який першим запропонував посилити колективну безпеку шляхом створення Ліги Націй, після Першої світової війни, він розробив План «14 пунктів» у 1918 році, що визначив концепцію колективної безпеки, як альтернативу війнам. Вільсон вважав, що міжнародні спори мають вирішуватися мирним шляхом, а агресія повинна викликати колективну реакцію.

Генрі Кіссінджер, американський дипломат і теоретик міжнародних відносин, який досліджував баланс сил і необхідність глобальної співпраці між

країнами, він наголошував, що колективна безпека повинна базуватися на реалістичних основах, де ключову роль відіграють великі держави. Значний внесок в теорію зробив Лестер Пірсон, лауреат Нобелівської премії миру, який сприяв ідеї миротворчих місій як інструменту колективної безпеки, він першим запропонував створити механізми для спільного реагування на конфлікти через ООН і Джозеф Най, автор концепції «м'якої сили» та стратегій кооперативної безпеки, що підкреслював важливість світових альянсів (НАТО, ЄС) як основи колективної безпеки в умовах глобалізації.

Реалізація концепції колективної безпеки відбувається через діяльність Організації Об'єднаних Націй (ООН), статут якої закріплює принцип колективної безпеки у главі VII («Дії щодо загроз миру»). Рада Безпеки ООН має право застосовувати санкції, миротворчі операції та військові заходи проти агресора. Наступним інститутом, що реалізує ідею колективної безпеки є НАТО (Організація Північноатлантичного договору), яка у статті 5, Північноатлантичного договору, закріплює принцип «колективного захисту», тобто напад на одну країну-члена розглядається як напад на всіх [3].

Міжнародні інститути визнали кібербезпеку, як п'ятий операційний простір для колективного реагування. Європейський Союз, в цьому напрямі, розробив Спільну політику безпеки та оборони (CSDP), яка передбачає координацію країн-членів у відповідь на загрози, включаючи кібербезпеку. Є цілий ряд глобальних та регіональних ініціатив, що підтримують і реалізують концепцію колективної безпеки, а саме, Будапештський меморандум у1994 році частково відображав спробу забезпечити колективну безпеку України, Шанхайська організація співробітництва, це регіональне об'єднання для протидії загрозам у Центральній Азії.

В умовах цифровізації концепція колективної безпеки поширюється на кіберзагрози, у зв'язку з чим, розроблено Кібердоктрину НАТО, як спільну відповідь на кібератаки як на традиційні військові загрози, є ряд інших глобальних ініціатив, розробка міжнародних норм та угод щодо кібербезпеки.

Отже, концепція колективної безпеки є фундаментальною основою міжнародного порядку, спрямованого на спільну протидію агресії, зокрема у сучасних умовах кіберзагроз.

Набирає популярності і прибічників теорія глобального управління, згідно з якою, держави, міжнародні організації, інститути громадянського суспільства та приватний сектор мають спільно формувати глобальні механізми кіберрегулювання, через координацію діяльності, обмін інформацією, розробку спільної стратегії. Теорія глобального управління (Global Governance) стосується механізмів, процесів та інститутів, які забезпечують спільне управління глобальними проблемами у сучасному світі.

Глобальне управління – це сукупність норм, правил, інститутів та процесів, що регулюють взаємодію держав і недержавних акторів у відповідь на глобальні виклики. Теорія виходить з ідеї, що жодна країна не може самостійно подолати глобальні проблеми, такі як зміна клімату, тероризм, економічні кризи або кіберзагрози. Отже, таке управління має бути мультиакторним, що передбачає участь держав, міжнародних організацій, приватних корпорацій, НУО та громадянського суспільства, поліцентричним, розподілення владних повноважень на глобальному, регіональному та національному рівнях [4].

Воно передбачає наявність глобальних норм, створення правил і стандартів для врегулювання міжнародних відносин, добровільність та кооперація у прийнятті управлінських рішень, співпрацю, яка базується на консенсусі, а не примусі. Теорія глобального управління поєднує ліберальний інтернаціоналізм та конструктивізм, які наголошують на можливості кооперації та значенні міжнародних інститутів у подоланні викликів. Представниками теорії глобального управління є Джеймс Розенау, він вважає, що світовий порядок стає більш децентралізованим і складним, де глобальне управління базується на взаємодії різних акторів – держав, корпорацій та інститутів.

Іншими відомими представниками теорії глобального управління є Джозеф Най, виходив з того, що в сучасному світі управління потребує

об’єднання «жорсткої» та «м’якої сили» для забезпечення глобальної стабільності, Дейвід Хелд, вважав, що глобальне управління потребує демократичної участі всіх акторів, включаючи громадянське суспільство та менш розвинені країни, Амартія Сен, Лауреат Нобелівської премії з економіки, підкреслює роль глобального управління у вирішенні проблем нерівності, бідності та людського розвитку [5].

Механізми реалізації глобального управління включають створення центральної платформи для вирішення глобальних проблем через консенсус, це передбачає активізацію світової організації торгівлі, для регулювання глобальної економічної політики, координацію економічної допомоги та стабільності за допомогою МВФ і Світового банку, розширення регіональних ініціатив Європейського Союзу, АСЕАН, створення інститутів регіонального глобального управління.

Велику роль вони вбачають в розвитку публічно-приватного партнерства, розширенні участі корпорацій та громадських організацій у вирішенні глобальних викликів (наприклад, у кібербезпеці чи кліматичній політиці), проведення глобальних форумів G7, G20, Всесвітніх економічних форумів, які об’єднують світових лідерів для узгодження політики. Критики цієї теорії апонують до домінування великих держав у прийнятті рішень, підкреслюють недостатню спроможність організацій (наприклад, ООН) реагувати на кризи, акцентують увагу на відмінностях між національними та глобальними пріоритетами, визначають неможливість цих ідей подолати технологічні виклики, забезпечити кібербезпеку та регулювання глобального Інтернет-простору [6].

Теорія національного інтересу, яка виходить з того, що тільки національні інтереси формують основу для прийняття рішень щодо внутрішніх та зовнішніх викликів, а також виступають інструментом обґрунтування дій у глобальному середовищі. На думку прибічників теорії, національні інтереси – це стратегічні цілі держави, спрямовані на забезпечення її суверенітету, безпеки, економічного розвитку та культурної ідентичності. Отже, концепція відображає

егоїстичний інтерес держави в міжнародній системі, де кожен актор діє для досягнення власної вигоди.

На першому місці у політиці має бути захист суверенітету, незалежності та територіальної цілісності, пріоритет економічних інтересві, доступ до ресурсів, торгівля, забезпечення безпеки, створення оборонної стратегії, збереження національної ідентичності та культурної спадщини. Представники концепції національних інтересів Нікколо Макіавеллі, Томас Гоббс, Ганс Моргентау, Карл Шмітт.

Реалізують концепцію національних інтересів Сполучені Штати Америки через зовнішню політику, в якій закладено захист економічних інтересів, боротьбу з тероризмом та утримання глобального лідерства, Китай, який здійснює захист економічного зростання через ініціативу *«Один пояс, один шлях»*. Україна теж стала на захист територіальної цілісності, просуває ідею інтеграції до ЄС і НАТО, посилює кібербезпеку та енергетичну незалежність, що є ключовими національними інтересами [7].

Сьогодні, на адресу цієї теорії звучить багато критики, аргументами виступає теза, що традиційні національні інтереси стикаються з глобальними викликами, виникає конфлікт інтересів, тобто суперечності між державами призводять до конфліктів, в сфері кібербезпеки національні інтереси реалізуються у новій формі через технологічні загрози. Сучасна політика продовжує реалізовувати національні інтереси в умовах глобалізації та нових викликів, таких як кіберзагрози та геополітична конкуренція.

Концепція цифрового суверенітету стосується стратегічного підходу держав, організацій та суспільства до цифровізації як ключового пріоритету для розвитку економіки, безпеки, освіти та державного управління, вона наголошує на необхідності ставити цифрові технології та інновації на чільне місце в політиці та стратегії розвитку. Цифровий пріоритет – це стратегічна орієнтація на використання цифрових технологій для прискорення економічного та соціального розвитку, забезпечення національної безпеки та конкурентоспроможності. Нею передбачається впровадження цифрових

технологій у всі сфери життя, пріоритетне фінансування та розвиток цифрової інфраструктури, акцент на цифрову безпеку, кіберзахист та технологічний суверенітет, створення умов для цифрової трансформації бізнесу, держави та суспільства [8].

Представники теорії виходять з того, що потрібно створити цифрову державу, де послуги надаються громадянам через цифрові платформи, прикладом є електронний уряд в Естонії або «Дія» в Україні. Потрібно побудувати цифрову економіку, орієнтовану на розвиток інновацій, стартапів, штучного інтелекту, хмарних обчислень, блокчейну та інших технологій, як Китайська програма «Made in China 2025». Цифровий суверенітет передбачає підтримку власної технологічної незалежності від зовнішніх гравців, створення національних платформ для зберігання даних, розвиток цифрової грамотності та освіти, навичок роботи з цифровими інструментами серед населення та кібербезпеку, забезпечення захисту інформаційних систем і критичної інфраструктури від кібератак.

Представники Клаус Шваб, автор концепції Четвертої промислової революції, його ключові тези, це те що цифрові технології (AI, IoT, Big Data) є основою для нової ери економічного та соціального розвитку, Томас Фрідман, вважає, що цифровізація та інтернет є ключовими рушіями глобальних змін, Джеффрі Сакс, виходить з того, що цифрові технології повинні стати пріоритетом для досягнення Цілей сталого розвитку (SDGs) ООН, Джефф Безос, засновник Amazon, який наголошував на цифрових інноваціях як основі бізнес-моделей нового покоління, Микола Федоров та «Дія», показав і розвинув український підхід до цифрової трансформації державних послуг через створення порталу «Дія»[9].

Основними напрямами реалізації теорії цифрового пріоритету є розвиток цифрової інфраструктури, інтернет покриття 5G, дата-центрів, національних хмарних рішень, інвестиції у R&D (дослідження та розробки), розвиток штучного інтелекту, квантових обчислень та інноваційних технологій, цифрової освіти, підготовка спеціалістів у галузі технологій, захист критичної

інфраструктури та збереження даних. Концепція цифрового пріоритету формує основу для стратегічного розвитку сучасних держав та компаній, орієнтованих на інновації та цифрові технології. Держави прагнуть захистити свої кіберкордони та контролювати критичну інфраструктуру, водночас міжнародна співпраця стає необхідною для протидії транснаціональним загрозам.

1.2. Особливості міжнародної співпраці в умовах глобалізації загроз в кіберпросторі

У сучасному світі кіберпростір став критично важливим середовищем, де взаємодіють держави, корпорації та окремі особи. Глобалізація кіберзагроз обумовлюється інтернаціоналізацією технологій, відкритістю цифрового середовища та швидким розвитком кіберзлочинності й кібератак. Це створює нові виклики для міжнародної співпраці, потребуючи координації зусиль на глобальному, регіональному та двосторонньому рівнях.

Посилився транскордонний характер загроз, це означає, що кібератаки не мають географічних меж та можуть завдати шкоди будь-якій країні світу, має місце анонімність кіберпростору, складність ідентифікації атакуючої сторони робить боротьбу з кіберзагрозами складною. Країни знаходяться в технологічній нерівності, вони мають різний рівень розвитку цифрової інфраструктури та можливостей захисту між країнами, заважає взаємозалежність інфраструктур, існуючі глобальні ланцюги поставок, енергосистеми та фінансові мережі, які вразливі до кібератак [10].

Ключовими глобальними загрозами став кібертероризм, використання цифрових технологій для дестабілізації суспільств і урядів, систематично відбувається кібершпигунство, іде викрадення даних державного та корпоративного значення, зросла кіберзлочинність, фінансові шахрайства, атаки на критичну інфраструктуру. Зростає дезінформація, поширюються фейкові новини для впливу на громадську думку, мають місце зловживання

технологіями штучного інтелекту для створення автоматизованих кібератак. Тому, міжнародна співпраця, в умовах глобалізації кіберзагроз, має ряд особливостей реалізації і організації.

Через глобальний характер загроз співпраця виходить за межі національних кордонів, отже, держави об'єднують зусилля для обміну інформацією, створюють спільні стратегії та розробляють інноваційні інструменти протидії. Розроблена Будапештська конвенція про кіберзлочинність (2001) – перший міжнародний договір, спрямований на боротьбу з кіберзлочинами, проведено глобальний форум з кіберекономічної безпеки (GFCE), в результаті чого створено міжнародний майданчик для обговорення кіберзахисту. Також, відбувається інституціоналізація співпраці через створення спеціалізованих міжнародних організацій та альянсів для координації дій у кіберпросторі. Так, за допомогою НАТО було створено Центр передового досвіду з кібероборони в Естонії, Агентство Європейського Союзу з кібербезпеки, Глобальний кіберцентр для боротьби з кіберзлочинністю при Інтерполі [11].

Посилюється значення публічно-приватного партнерства (PPP) в контексті співпраці між державами та приватним сектором, що є необхідним, адже більшість інфраструктури кіберпростору перебуває у власності приватних компаній. Корпорації, такі як Microsoft, Google та Cisco, відіграють ключову роль у протидії загрозам, Microsoft Digital Crimes Unit – підрозділ для боротьби з глобальними кіберзагрозами. Основним елементом співпраці є швидкий обмін інформацією про кіберінциденти для мінімізації збитків, адже, спільний доступ до технологій дозволяє підвищувати рівень кіберзахисту на глобальному рівні.

Формуються національні команди реагування, що співпрацюють у глобальній мережі, іде розробка міжнародних стандартів і норм, так як, умови глобалізації вимагають розробки універсальних правил поведінки у кіберпросторі для держав та недержавних акторів. Але країни стикаються з масштабними викликами, що посилює суперечності між ними щодо регулювання та суверенітету у кіберпросторі. Тому, група урядових експертів

ООН розробила ініціативу щодо формування правил поведінки у кіберпросторі, для подолання конфлікту інтересів і покращення кібергеополітики.

Співпраця ускладнюється через різні політичні інтереси держав та відсутність глобального регулювання, так великі держави, як-от США, Китай і Росія, часто конкурують за вплив у цифровому середовищі, посилюється протистояння США-Китай у сфері технологічного суверенітету та 5G-інфраструктури. Таким чином, виникає потреба урізноманітнювати форми міжнародної співпраці, заключати двосторонні угоди між країнами щодо обміну інформацією та спільної боротьби з кібератаками. Через міжнародні альянси, такі як НАТО, ЄС, ОБСЄ, потрібно об'єднати країни для розробки стратегій кіберзахисту.

Такі заходи мінімізують виклики міжнародної співпраці в кіберпросторі, зменшать недовіру між державами, підозри у кібершпигунстві та атаках. Відсутність єдиних міжнародних норм щодо поведінки у кіберпросторі, анонімність атакуючих сторін, складність атрибуції відповідальності, технологічна нерівність, розрив між розвиненими та менш розвиненими країнами, це теж виклики, які потрібно долати. Міжнародна співпраця в умовах глобалізації загроз у кіберпросторі є критично важливою для забезпечення стабільності, безпеки та розвитку у цифрову епоху. Особливості такої співпраці включають транскордонний характер загроз, необхідність публічно-приватного партнерства, інституціоналізацію зусиль та розробку міжнародних стандартів. Однак конфлікт інтересів, відсутність єдиних правил та технологічна нерівність продовжують створювати перешкоди на шляху до ефективної глобальної координації у кіберсфері [12].

Не менш важливо дотримуватись принципів міжнародної співпраці у сфері кібербезпеки, суверенної рівності держав, це основний принцип на якому базується міжнародна співпраця на рівноправності учасників. Добровільність та взаємна вигода, означає, що держави беруть участь у ініціативах з урахуванням власних інтересів, прозорість і довіра – відкритий обмін інформацією та розвиток довіри між партнерами, спільна відповідальність, тому що глобальні

кіберзагрози вимагають колективної відповіді, дотримання міжнародного права, так, співпраця повинна відповідати нормам міжнародного гуманітарного права та кіберправа.

Міжнародно-правовими засадами співпраці у сфері кібербезпеки є Будапештська конвенція про кіберзлочинність (2001 р.), перший міжнародний договір, що регулює протидію кіберзлочинності, Резолюції ООН з питань кібербезпеки, яка закликає до міжнародної співпраці у протидії кіберзагрозам, Директиви ЄС (NIS Directive), що встановлюють вимоги для кібербезпеки критичної інфраструктури країн-членів, Доктрини та стратегії НАТО, які підкреслюють кіберзахист як основний елемент оборони альянсу. Основними формами міжнародної співпраці є двосторонні угоди, це співпраця між окремими державами щодо обміну даними та досвідом, регіональні ініціативи, це спільні стратегії країн одного регіону (наприклад, ЄС, ОДКБ), глобальні форуми, публічно-приватне партнерство через залучення приватних компаній для підвищення кіберзахисту [13].

ВИСНОВОК ДО РОЗДІЛУ 1

Теоретичні засади міжнародної співпраці у сфері кібербезпеки базуються на глобальних принципах безпеки, суверенітету, прозорості та колективної відповідальності. Спільна діяльність держав, міжнародних організацій і приватного сектору є ключем до створення ефективного механізму реагування на сучасні кіберзагрози. У сучасних умовах глобалізації кіберзагрози не визнають державних кордонів, що робить міжнародну співпрацю ключовим елементом ефективної протидії кіберзлочинності.

Координація зусиль між державами, міжнародними організаціями та приватним сектором є необхідною для забезпечення глобальної кібербезпеки. Відсутність єдиних міжнародних стандартів у сфері кібербезпеки створює бар'єри для ефективної співпраці, тому це стає важливим завданням

гармонізації національного законодавства з міжнародними нормами, такими як Будапештська конвенція про кіберзлочинність. Організації, як-от ООН, НАТО, ЄС та Інтерпол, відіграють важливу роль у координації зусиль, розробці стандартів і забезпеченні обміну інформацією між країнами. Їхні ініціативи сприяють створенню ефективних механізмів для запобігання та розслідування кіберзлочинів. Особливу увагу в міжнародній співпраці приділяють захисту критичних об’єктів, таких як енергетичні системи, банківські мережі та транспортні комунікації. Спільні програми з обміну технологіями та досвідом значно підвищують рівень їхньої захищеності.

Важливим аспектом міжнародної співпраці є обмін оперативними даними та розвідувальною інформацією. Проте це часто ускладнюється через питання конфіденційності, довіри та різницю у правових системах. Розвиток кібердипломатії є новим напрямом міжнародної співпраці. Це включає переговори про угоди щодо кібербезпеки, розробку міжнародних стандартів поведінки в кіберпросторі та врегулювання кіберконфліктів. Приватні компанії володіють значними ресурсами та експертизою у сфері кібербезпеки. Їх залучення до міжнародних програм сприяє розробці інноваційних рішень і створенню глобальної екосистеми кіберзахисту.

РОЗДІЛ 2.
ОЦІНКА СТАНУ МІЖНАРОДНОЇ ВЗАЄМОДІЇ УКРАЇНИ В УМОВАХ ЗРОСТАННЯ КІБЕРЗАГРОЗ

2.1. Аналіз викликів та механізмів управління кібербезпекою в Україні

Україна є однією з країн, яка найбільше піддається кіберзагрозам через свою геополітичну ситуацію, конфлікт із Російською Федерацією та стратегічне розташування. У цьому контексті, міжнародна взаємодія в сфері кібербезпеки стала необхідною компонентою національної стратегії захисту. Тому, оцінка стану, досягнень та викликів міжнародної співпраці України в умовах зростання кіберзагроз є вкрай актуальною, особливо під час війни. Основні виклики, у сфері кібербезпеки України, пов'язані з гібридною війною та агресивною роллю росії, яка активно використовує кіберзасоби для впливу на Україну, включаючи атаки на інфраструктуру, дезінформаційні кампанії та шкідливе програмне забезпечення.

Масштабні кібератаки, в тому числі на енергетичну систему України, показали високий рівень організації та спрямованості цих дій. Агресор використовує вразливість критичної інфраструктури України, низький рівень цифрової грамотності у деяких галузях, обмеженість ресурсів для модернізації систем захисту. Значно погіршує ситуацію недостатній рівень міжнародної координації, відсутність оперативного обміну даними про кіберзагрози між Україною та окремими партнерами та нерівномірний рівень підготовки українських спеціалістів до співпраці із закордонними структурами [14].

Разом з тим, Україна має суттєві досягнення у сфері міжнародної взаємодії через активну співпрацю з НАТО, через розробку і реалізацію програм з кіберзахисту, створення платформи Cooperative Cyber Defence Centre of Excellence. На цій платформі відбуваються навчання та тренінги для українських фахівців, а також консультації щодо підвищення стійкості до

кібератак. Також, Україна розширила партнерство з Європейським Союзом, а саме, заключила Угоду про кіберзахист як частину Угоди про асоціацію між Україною та ЄС, прийняла участь у програмі Horizon Europe, яка включає підтримку інновацій у сфері кібербезпеки.

Є багато двосторонніх домовленостей з важливими, для Україн, країнами, договір про **с**півпрацю з США, в рамках стратегічного партнерства, включаючи програми технічної допомоги та обмін інформацією, угода з Естонією щодо обміну досвідом у побудові кіберрезерву та кіберполітики. Швидкими темпами відбувається інтеграція у міжнародні спільноти, країна приймає **у**часть у спільноті FIRST, що забезпечує доступ до глобальної мережі експертів, співпрацює з ITU (Міжнародним союзом в сфері електрозв'язку), у проєктах кіберзахисту.

Україна бере участь в ООН-ких дискусіях щодо норм поведінки держав у кіберпросторі, взаємодіє з групою урядових експертів ООН та Відкритою робочою групою з кібербезпеки. Заключено ряд двосторонніх угод зі США, в рамках Стратегічного партнерства, що включають підтримку у сфері кібербезпеки, а також, програм обміну досвідом між Кіберкомандуванням США та українськими структурами. Відбувається співпраця з Великою Британією у галузі кібернавчань, консультацій та розслідувань кіберінцидентів, з Ізраїлем досягнуто підписання угоди про партнерство у розробці технологій кіберзахисту та штучного інтелекту, для протидії загрозам [15].

Досягненням України є покращення законодавства, так, прийнятий закон України «Про основні засади забезпечення кібербезпеки України» у 2017 році, став базою для системних змін законодавчого поля та створення інституцій. Сьогодні активізувалась діяльність Національного координаційного центру з кібербезпеки при РНБО, який забезпечує інтеграцію у світові платформи, відбулось приєднання до міжнародної платформи *No More Ransom* для боротьби з програмами-вимагачами, на базі центру проводяться регулярні тренінги та симуляції для співробітників державних органів.

Незважаючи на фрагментарність дій між окремими міжнародними та внутрішніми структурами та відсутність чіткого кібердипломатичного вектору, Україна активно ініціює обговорення кібербезпеки на міжнародних майданчиках. Ми вже маємо важливі досягнення у сфері кібербезпеки, але для ефективного протистояння зростаючим кіберзагрозам необхідно зміцнити міжнародну співпрацю через активну дипломатію, інновації та інтеграцію в глобальні ініціативи.

Інституційна структура кіберзахисту в Україні представлена Радою національної безпеки і оборони (РНБО), що відповідає за стратегічне планування у сфері кібербезпеки, здійснює координацію діяльності через Національний координаційний центр з кібербезпеки. Національний координаційний центр кібербезпеки – це орган, створений при Раді національної безпеки і оборони України для координації дій у сфері кібербезпеки, його основними завданнями є аналіз, планування та координація заходів для захисту кіберпростору України. Основні функції Національного координаційного центру кібербезпеки України полягають у аналітичній діяльності, моніторингу та аналізу кіберзагроз, відстеженні поточних і нових загроз у кіберпросторі, аналізі тенденцій та джерел атак, оцінці кіберризиків, визначенні вразливостей у критичній інформаційній інфраструктурі [16].

Значне місце в діяльності центру займає розробка сценаріїв можливих атак та їхнаслідків, координація між органами влади, СБУ, кіберполіцією, Мінцифри, Міністерством оборони формування і впровадження кіберполітики. За допомогою центру узгоджуються стратегії і плани дій у сфері кіберзахисту, готуються рекомендації для уряду та президента, здійснюється захист критичної інформаційної інфраструктури. Обов’язками центру є розробка та запровадження сучасних стандартів безпеки та регламентів з метою інтеграції у світову кіберекосистему.

З моменту створення, Національний координаційний центр активно взаємодіє з НАТО, ЄС, та іншими міжнародними партнерами, ним організовується обмін даними про кіберзагрози з міжнародними організаціями

та державами-партнерами. Також, обов'язком центру є розробка нормативно-правових актів, імплементація міжнародних стандартів та впровадження рекомендацій і норм НАТО, ENISA (Агентства ЄС з кібербезпеки) та інших організацій, він здійснює підготовку пропозицій щодо змін у законодавстві для підвищення ефективності кібербезпеки.

Основними завданнями НКЦК, у контексті стратегії кібербезпеки України, є координація між державними та приватними структурами, захист національних інтересів у кіберпросторі, впровадження інноваційних технологій у системи кіберзахисту, створення умов для співпраці з міжнародними партнерами, забезпечення кіберстійкості критичних систем і об'єктів інфраструктури. Отже, Національний координаційний центр кібербезпеки є центральною ланкою у створенні надійної системи кіберзахисту в Україні, забезпечуючи як оперативне реагування на загрози, так і стратегічне планування у сфері кібербезпеки.

Значну роль у виявленні і протидії кіберзагрозам виконує служба безпеки України (СБУ), вона веде розслідування в сфері кіберзагроз, так як вони становлять загрозу національній безпеці, Міністерство цифрової трансформації, яке займається цифровізацією, впровадженням технологій кіберзахисту у державному секторі та створенням програм з підвищення обізнаності про кібербезпеку, кіберполіція, що відповідає за боротьбу з кіберзлочинністю, розслідування інцидентів [17].

Спільно з органами влади ці інститути ведуть розробку та впровадження національної системи захисту електронних ресурсів, яка сприяє зміцненню та захисту критичної інфраструктури, впроваджують сучасні стандарти безпеки. Ці дії супроводжуються розширенням публічно-приватного партнерства для захисту інфраструктури та збільшенням фінансування. Представлені механізми показують, що Україна має значний потенціал для покращення кібербезпеки, але потребує інтегрованого підходу, який об'єднує зусилля державних органів, приватного сектора, громадськості та міжнародних партнерів.

2.2. Проблеми організації міжнародної співпраці України в сфері кібербезпеки

Агрессор активно використовує кіберпростір для дестабілізації України, веде атаки на енергетичну інфраструктуру, фінансовий сектор, проводить постійні інформаційні кампанії для втручання у внутрішні справи, зокрема під час виборів та кризових ситуацій. Україна мусить відбивати атаки з боку цілих хакерських угруповань, які використовують країну як «транзитний майданчик» для операцій, зростають атаки програмам-вимагачів та фішинг-кампаній.

Відбувається використання передових методів атак, включно з шкідливим програмним забезпеченням, соціальною інженерією, штучним інтелектом. При відсутності єдиного центру управління, ускладнюється координаціє між державними органами, різні державні інституції мають дублюючі або перетинаючі функції (РНБО, СБУ, Мінцифра, поліція). Брак коштів не дає можливості провести модернізацію систем кіберзахисту і зробити інвестиції у технології кібербезпеки. Крім того, недостатня кількість висококваліфікованих фахівців у сфері кібербезпеки і війна викликала значний відтік кадрів у приватний сектор або за кордон [18].

Вразливість зростає через неналежне використання базових засобів захисту, таких як оновлення програмного забезпечення або використання складних паролів, найбільш вразливі енергетичні, транспортні, фінансові і телекомунікаційні системи. Причиною є відсутність сучасних стандартів безпеки у багатьох секторах і недотримання норм Законів «Про основні засади забезпечення кібербезпеки України» та «Про захист інформації в інформаційно-телекомунікаційних системах», повільне впровадження міжнародних стандартів (ISO 27001).

Під час війни, вагомою проблемою є нестача фінансування для забезпечення сучасних систем кіберзахисту, обмежений людський потенціал у вигляді кваліфікованих спеціалістів, цілий ряд бюрократичних бар'єрів, а саме, тривалі процедури ухвалення міжнародних угод, недостатній рівень адаптації

українського законодавства до стандартів ЄС і НАТО. Україна стикається з технічними викликиами, так, має місце швидкий розвиток методів атак у порівнянні з повільними темпами впровадження захисту, відсутня єдина платформа для обміну інформацією про інциденти. Багато розмов і рішень відносно гармонізації національного законодавства зі стандартами ЄС та НАТО та створенням механізмів швидкого реагування на кіберінциденти на міжнародному рівні, але вони недостатньо результативні.

Незважаючи на складні умови реалізації політики держави в сфері кібербезпеки, в умовах війни, Україна значні кошти інвестує в людський капітал, у підготовку висококваліфікованих фахівців, збільшуючи їх участь у міжнародних програмах, залучає гранти та технічну допомогу для освітніх проєктів у сфері кібербезпеки. Можна говорити про інтеграцію у нові міжнародні ініціативи, участь у проектах глобального моніторингу кіберзагроз та розширення співпраці із країнами Азії та Близького Сходу, які демонструють високий рівень розвитку кіберзахисту. Посилюється оперативний обмін інформацією**,** створюються спільні центри моніторингу кіберзагроз із країнами-партнерами, впроваджуються міжнародні стандарти обміну даними, такі як STIX/TAXII.

Отже, Україна демонструє прогрес у зміцненні міжнародної взаємодії у сфері кібербезпеки, але стикається з низкою викликів, які потребують подальшого вирішення. Посилення співпраці із західними партнерами, розвиток людського капіталу та інтеграція до міжнародних структур, допомагають країні забезпечити кіберстійкість, навіть під час війни. Не зважаючи на використання росією кіберпростору для дестабілізації ситуації в Україні, постійні атаки на критичну інфраструктуру, інформаційні кампанії та розвідувальні операції кібербезпека країни посилюється [19].

В цій сфері пріоритетом номер один є співпраця з міжнародними організаціями, як уже підкреслювалось, Україна бере участь у програмах кібербезпеки НАТО, зокрема через Платформу довіри кіберзахисту, постійно проводить спільні навчання (наприклад, *Cyber Coalition*), що дозволяє

покращувати готовність до відбиття атак. Особливо активно відбувається співробітницьво з ЄС, так, Україна бере **у**часть у програмі *EU Cyber Capacity Building*, що спрямована на підвищення кіберстійкості та співпрацює з Європолом та ENISA (Агентство ЄС із кібербезпеки) для боротьби з кіберзлочинністю. Організація міжнародної співпраці України в сфері кібербезпеки є важливим завданням, враховуючи зростання кількості кіберзагроз і стратегічне значення кіберпростору.

Актуальною проблемою є недостатня правова база, Україна дуже повільно адаптує своє законодавство до міжнародних стандартів, імплементація норм ЄС у сфері захисту даних та кібербезпеки перебуває на ранніх стадіях, є значна невідповідність національних законів сучасним викликам, пов’язаним із кіберзагрозами. Нажаль залишається низьким рівень міжнародної довіри, так, Україна стикається з проблемою недовіри з боку деяких міжнародних партнерів, через корупцію та відсутність прозоррсті у сфері реалізації проєктів, недостатнім є рівень участі України у ключових міжнародних альянсах і структурах кіберзахисту [20].

Україна недостатньо інтегрована у великі міжнародні програми, спрямовані на розвиток кібербезпеки і має низьеу участь у міжнародних навчаннях та симуляціях кіберінцидентів. Частіше це відбувається в результаті низького рівня обміну інформацією, тому, що нендостатньо розвинена система обміну даними про кіберзагрози з міжнародними партнерами і є кладнощі у координації із приватним сектором, що володіє значними ресурсами для боротьби з кіберзагрозами.

Отже, для вирішеннь представлених проблем потрібно зміцнити законодавчу базу, через гармонізацію з міжнародними стандартами, розширити міжнародне співробітництво через участь у глобальних кібербезпекових альянсах та програмах. Потрібно також, інвестувати у розвиток людського капіталу через навчальні програми і тренінги для спеціалістів, залучити міжнародну технічну допомогу, зокрема через програми ЄС, НАТО, та інших партнерів, розробити національну стратегію кібербезпеки, яка враховуватиме

міжнародні аспекти і допоможе Україні зміцнити свої позиції у сфері кібербезпеки на міжнародній арені. Вкрай важливо забезпечити кіберзахист посадових осіб, знайти інструменти їх кібербезпеки, рис. 2.1.[21].

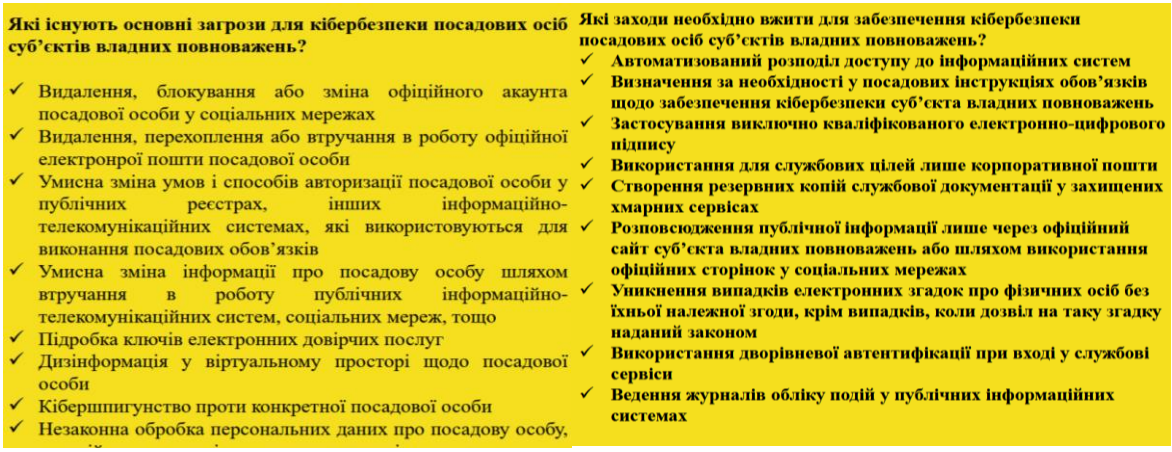

Рис. 2.1. Основні загрози і заходи забезпечення кібербезпеки посадових осіб

Джерело: [21].

Як видно з рис. 2.1., є значна кількість загроз в сфері кібербезпеки посадовців, які можуть викликати блокування і зміну їх офіційних акаунтів, привести до втручання в їх діяльність, взагалі змінити інформацію про посадовця, обробити їх персональні дані. Таким чином, потрібно відповідним інститутам застосувати ряд заходів по забезпеченню кібербезпеки влади.

ВИСНОВКИ ДО РОЗДІЛУ 2

У контексті значного зростання кіберзагроз, Україна активно інтегрується в міжнародну систему безпеки, зосереджуючи зусилля на партнерстві з розвиненими країнами, міжнародними організаціями та спеціалізованими установами. Співпраця з НАТО, ЄС, ОБСЄ та ООН є ключовими напрямами зміцнення кібербезпеки держави. Здійснюються суттєві кроки в розвитку національних інституцій для протидії кіберзагрозам, зокрема створення Державної служби спеціального зв'язку та захисту інформації (ДССЗЗІ), кіберполіції та інших органів. Ці інституції активно співпрацюють із

міжнародними партнерами у сфері обміну досвідом та технологіями. Україна є активним учасником глобальних ініціатив, таких як Будапештська конвенція про кіберзлочинність, програми ЄС «Цифровий ринок» та ініціативи з розвитку кібердіпломатії. Це сприяє гармонізації національного законодавства з міжнародними стандартами та залученню технічної допомоги.

Завдяки міжнародній підтримці Україна реалізує програми із захисту критичних об’єктів, таких як енергетична, фінансова та інформаційна інфраструктура. Особливу роль відіграють спільні навчання, проведені за участі НАТО та партнерських держав. Попри значний прогрес, залишаються проблеми, пов’язані з обмеженістю фінансових ресурсів, недостатньою координацією між національними структурами та інституціями, а також складністю забезпечення оперативного обміну інформацією із міжнародними партнерами. Приватний сектор та неурядові організації дедалі активніше залучаються до ініціатив у сфері кібербезпеки. Проте їхня інтеграція в міжнародні програми потребує більш структурованого підходу з боку держави.

РОЗДІЛ 3.
СТРАТЕГІЧНІ НАПРЯМИ ПОСИЛЕННЯ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА В СФЕРІ КІБЕРБЕЗПЕКИ

3.1. Побудова міжнародної стратегії реагування на кіберзагрози

Сучасна стратегія кібербезпеки в Україні спрямована на визначення пріоритетів, цілей та завдань для забезпечення захисту від кіберзагроз, щоб сформувати умови безпечності діяльності і відносин у кіберпросторі і його використанні для реалізації інтересів окремих осіб, суспільства в цілому та державних інститутів. Подолання кіберзагроз це основний пріоритет в системі національної безпеки держави, реалізація якого має здійснюватись через удосконалення спроможностей національних інститутів кібербезпеки.

Формування нової Стратегії кібербезпеки України враховує світові та глобальні виклики у глобальному кіберсередовищі, та їх вплив на розвиток національної екосистеми, рис. 3.1. [22].

Рис. 3.1. Українська стратегія кібербезпеки

Джерело: [22].

Як видно з рис. 3.1., стратегія та політика України подолання кіберзагроз об’єднує уряд, приватний сектор, громадянське суспільство і науку.Основними суб’єктами, які несуть відповідальність за кібербезпеку є Рада національної безпеки і оборони і Національний центр кібербезпеки. Останнім часом ризики, пов'язані з кіберпростором України, стали набагато серйознішими. Зокрема, так звані «цілеспрямовані кібератаки» спрямовані на викрадення конфіденційної інформації, що стосується національної безпеки та ключових технологій. Росія масово застосовує кібератаки на об'єкти критичної інфраструктури, що завдає серйозної шкоди економічній і соціальній діяльності, крім того, поширення ІКТ з розширеними функціями призвело до кібератак на енергетичну інфраструктуру, а також окремих осіб та організації. Ризики зараз швидко поширюються за межі кордонів окремих областей і регіонів і стають все більш всеохоплюючими [31].

Таким чином, кібератаки в всеукраїнському масштабі стали «спільними ризиками» з якими стикаються всі країни. Міжнародна співпраця стала необхідною для того, щоб вжити заходів проти цих «спільних атак», які завдають

завдають шкоди у всьому світі. У відповідь на ці мінливі умови уряд України постійно зосереджуєувагу світової спільноти на необхідності міжнародної стратегії співпраці в галузі кібербезпеки, яка ініційована Радою з нацональної безпеки і оборони України. Оскільки кіберзагрози стають нагальним глобальним викликом, що стоїть перед міжнародним співтовариством в цілому, важливо визнавати різні цінності, будувати взаємну довіру та працювати пліч-о-пліч для протидії викликам, щоб країни світу могли співіснувати в кіберпросторі та максимально використовувати його переваги. Україна рішуче налаштована на активне зміцнення співпраці та взаємодопомоги на міжнародному рівні, ми можемо похвалитись високим рівнем телекомунікаційної інфраструктури, значними досягненнями в цифровізації [23].

Завдяки зростаючому використанню і застосуванню інформаційно-комунікаційних технологій та гібрідною війною, Україна вже зіткнулась з різноманітними кіберзагрозами. Відповідно, країна прагне використовувати цей великий досвід і знання для сприяння міжнародному співробітництву. Міжнародна кібестратегія має спрямовувати політику всіх держав та їх пріоритетні напрями на посилення міжнародного співробітництва та взаємодопомоги у сфері кібербезпеки, щоб їх можна було представити у вигляді пакету дій.

Україна сприятиме всім ініціативам з міжнародного співробітництва і взаємодопомоги у сфері кібербезпеки на основі цієї стратегії в рамках спільного розуміння між усіма національними зацікавленими сторонами, в тому числі включаючи представників промисловості, наукових кіл та уряду. Вона буде активно сприятиме формуванню безпечного та надійного кіберпростору, в якому забезпечується вільний потік інформації шляхом розбудови відносин співробітництва з країнами по всьому світу. Основними принципами, які забезпечать результативність міжнародного співробітництва є забезпечення вільного потоку інформації, реагування на дедалі серйозніші ризики, посилення підходу, заснованого на оцінці ризиків і дії в партнерстві на основі соціальних та політичних зобов'язань, тобто соціальної відповідальності всіх зацікавлених сторін.

Зокрема, вкрай важливо підтримувати і розвивати безпечний і надійний кіберпростір, в якому забезпечується вільний потік інформації з метою забезпечення свободи вираження поглядів і активної політичної і економічної діяльності в кіберпросторі, сприяти інноваціям, економічному зростанню та вирішенню соціальних питань, а також для забезпечення позитивних переваг, якими можуть користуватися країни по всьому світу У міжнародній співпраці мають брати участь різні суб'єкти, такі як уряд, приватні компанії та науково-дослідні інститути. Для того, щоб зробити ці зусилля ефективними та послідовними, на основі дотримання основних принципів, описаних вище [24].

Міжнародна стратегія дасть можливість зміцнити міжнародне співробітництво та загальне глобальне розуміння необхідності розширення технологічних кордонів на глобальному рівні. Отже, питання, що стосуються кібербезпеки, широко варіюються в широкому спектрі, від соціально-економічних до національної безпеки. Існує також нескінченне розмаїття суб'єктів, які можуть брати участь у цьому процесі, і ступенів, до яких може бути досягнуто спільне розуміння викликів. Це спільне розуміння потрібно розвивати поступово, де це можливо, поважаючи при цьому різноманітні цінності.

З метою посилення поступового зміцнення спільного глобального взаєморозуміння кіберзагроз, як основної базової політики, Україна розробила телекомунікаційну інфраструктуру високого рівня, що призвело до збільшення використання та застосування кіберпростору різними суб'єктами. Під час повномасштабного вторгнення, вона зіштовхнулась з серйозними проблемами кібербезпеки, для відповідних структур як у державному, так і в приватному секторах, які сьогодні працюють в партнерстві над реалізацією широкого спектру заходів для вирішення цих проблем.

У просуванні зусиль міжнародного співробітництва важливо визначати пріоритетні напрямки для ефективної протидії різним проблемам кібербезпеки та максимального використання обмежених ресурсів. Міжнародна стратегія повинна визначати пріоритетні напрями, перш за все, впровадження систем динамічного реагування на кіберінциденти на основі удосконалення механізму міжнародного співробітництва та партнерства для глобального реагування на зростаючі кіберінциденти. На засадах розширення партнерства глобальне реагування сприятиме розширенню контролю за кіберпростором, створить фундамент для динамічного реагування на кіберінциденти, підвищить стандарти кібербезпеки базових спроможностей і механізмів реагування на глобальному рівні [35].

Розбудова основ динамічного реагування, яка спрямована на механізмів реагування на глобальному рівні, базується на удосконаленні міжнародної

нормотворчості у сфері кібербезпеки та підвищенні стандартів кібербезпеки. У міжнародному співробітництві виникають питання, які потребують спільного розуміння, але відрізняються в підходах країн та регіонів. Міжнародна стратегія

узагальнює необхідні заходи в країнах і регіонах, які мають тісні відносини з Україною, а також напрями українського впливу на багатосторонні структури. Міжнародна стратегія співробітництва у сфері кібербезпеки має роз'яснювати позиції кожної країни у цій сфері на двосторонньому, багатосторонньому та регіональному рівнях, спрямованих на прискорення зусиль в напряму міжнародного співробітництва щодо швидкого та належного реагування на кіберзагрози.

Інформаційно-комунікаційна інфраструктура Інтернету продовжує розвиватись, а її використання та застосування еволюціонує, неминуче, що питання кібербезпеки ставатимуть більш серйозними. Швидко і належним чином реагуючи на ці виклики шляхом тісної співпраці між відповідними організаціями, дасть можливість забезпечити безпечне використання кіберпростору.

3.2. Шляхи посилення протидії дезінформації і кіберзлочинності в умовах глобалізації

Попередній аналіз показав, що протидія дезінформації та кіберзлочинності в умовах глобалізації є критично важливою проблемою для національної безпеки, суспільної стабільності та ефективного функціонування державних і приватних інституцій. Основними шляхами посилення цих зусиль є розвиток правового регулювання, адаптація українського законодавства до світових стандартів та створення такої сучасної законодавчої бази, яка буде враховувати нові кіберзагрози і регулювати ступінь відповідальності за поширення дезінформації.

Для цього потрібна потужна міжнародна співпраця, укладання двосторонніх та багатосторонніх угод для боротьби з кіберзлочинами на глобальному рівні, регуляція платформ та запровадження вимог до соціальних медіа для швидкого реагування на дезінформацію та видалення шкідливого контенту. На рперше місце виходить впровадження передових технологій та використання штучного інтелекту, машинного навчання для виявлення кіберзагроз та дезінформаційних кампаній [34].

Технології мають бути орієнтовані на захист критичної інфраструктури, створення багаторівневих систем безпеки для захисту державних, енергетичних, фінансових та інших важливих систем. Отже, має відбуватись централізація кіберзахисту, створення національних центрів реагування на кіберзагрози та їх інтеграція з міжнародними партнерами. Другим важливим пріоритетом є розвиток медіаграмотності, проведення кампаній з підвищення обізнаності громадян про дезінформацію та способи її виявлення. Організація курсів для журналістів, правоохоронців і працівників ІТ-сфери щодо протидії дезінформації та кіберзлочинності теж стають важливим інструментом подолання кіберзагроз.

Потрібно популяризувати етичні норми поведінки в інтернеті, роз'яснювати важливість дотримання цифрової етики серед широких верств населення, впроваджувати фільтри для контенту, розробляти автоматизовані інструменти для ідентифікації фейкових новин та розпізнання шкідливого програмного забезпечення. Інтеграція технологій для швидкої нейтралізації шкідливих програм і бот-мереж та застосування блокчейн-технологій з використанням децентралізованих систем для перевірки джерел інформації [36].

Ініціативи мають носити глобальний характер, для цього Україна має брати участь у міжнародних форумах, таких як Глобальний форум кібербезпеки, та підтримувати ініціативи, проводити спільні операції з транснаціональних розслідувань та операції для ліквідації кіберзлочинних угруповань. Розвиток платформ для обміну розвідувальними даними між

державами, створення правдивих наративів, активне поширення правдивої інформації через офіційні канали та соціальні медіа, підтримка незалежних медіа теж пріоритетні шляхи посилення кібербезпеки.

Надання фінансової та технічної допомоги незалежним ЗМІ, які борються з дезінформацією, швидке реагування на спроби маніпуляції суспільною думкою через інформування громадськості, посилення діяльності правоохоронних органів, кіберполіції, масштабне розширення її повноважень і технічних можливостей підрозділів, що займаються кіберзлочинністю. Потрібно створити аналітичні групи і кіберкоманди для відстеження кіберзлочинців та аналізу інформаційних загроз з залученням публічно-приватного партнерства у співпраці правоохоронців з ІТ-компаніями та інтернет-провайдерами. Успіх протидії дезінформації та кіберзлочинності залежить від системного підходу, що поєднує технологічний, правовий, освітній і дипломатичний компоненти. Це потребує консолідації зусиль усіх зацікавлених сторін: уряду, бізнесу, громадянського суспільства та міжнародних партнерів.

ВИСНОВКИ ДО 3 РОЗДІЛУ

Ефективне міжнародне співробітництво у сфері кібербезпеки потребує створення єдиної глобальної архітектури, що базується на узгоджених стандартах, правилах і принципах поведінки в кіберпросторі. Україна має активно долучатися до розробки таких механізмів на базі міжнародних організацій, таких як ООН, НАТО та ОБСЄ. Узгодження національного законодавства з міжнародними стандартами, зокрема в рамках Будапештської конвенції, є важливим етапом інтеграції України до міжнародної кіберспільноти. Це сприятиме кращій координації зусиль у протидії кіберзлочинності.

Взаємодія з НАТО в межах програми «Партнерство заради миру» та участь у європейських ініціативах з кібербезпеки має стати одним із пріоритетів. Це дозволить Україні отримати доступ до сучасних стандартів захисту, навчань та технічної підтримки. Побудова ефективної системи обміну розвідувальними даними між країнами-партнерами є критично важливою для вчасного виявлення та нейтралізації кіберзагроз. Важливим завданням є забезпечення захищених каналів комунікації для такого обміну.

Міжнародне співробітництво потребує довіри між партнерами. Україна повинна дотримуватися прозорих стандартів, демонструвати готовність до відкритого діалогу та надавати достовірну інформацію. Розробка та впровадження міжнародної стратегії кібербезпеки, що інтегрує міжнародні програми, дозволить забезпечити стійкість і гнучкість у відповідях на глобальні виклики.

ВИСНОВКИ

Таким чином, Україна досягла помітного прогресу в налагодженні міжнародної взаємодії для протидії кіберзагрозам. Проте ефективність цих зусиль залежить від здатності держави долати внутрішні виклики, продовжувати модернізацію кібербезпеки та забезпечувати сталий розвиток партнерських відносин із міжнародною спільнотою. В умовах стрімкого зростання кіберзагроз міжнародна співпраця є стратегічно важливою для України. З огляду на складність та транснаціональність кіберзлочинності, партнерство із світовою спільнотою є ключовим інструментом для зміцнення національної кібербезпеки. Серед головних проблем виділяються:

- недостатній рівень інтеграції україни у глобальну систему кіберзахисту;
- обмеженість фінансових ресурсів і технологічної бази;
- відсутність повної гармонізації національного законодавства з міжнародними стандартами;
- проблеми оперативного обміну інформацією через обмеження доступу до сучасних технологій і інструментів захисту.

Україна активно співпрацює з міжнародними організаціями, такими як НАТО, ЄС, ОБСЄ, Інтерпол, та долучається до ініціатив на кшталт Будапештської конвенції. Ці зусилля сприяють розвитку інституційної спроможності, підвищенню рівня обізнаності та залученню технічної допомоги. Але, потрібно підвищувати кваліфікацію національних фахівців через спільні навчання, посилювати захист критичної інфраструктури завдяки обміну досвідом і практиками.

Для підвищення ефективності міжнародної співпраці у сфері кібербезпеки Україні слід зосередитися на таких стратегічних напрямках:

- гармонізація законодавства із міжнародними стандартами, зокрема в межах вимог ЄС та НАТО;

- розвиток кібердипломатії як інструменту для просування національних інтересів у сфері кібербезпеки;
- інтеграція з глобальними платформами обміну розвідувальною інформацією для своєчасного реагування на загрози;
- інвестиції у дослідження та інновації, які дозволять протистояти новим викликам у кіберпросторі.

Україна повинна активніше залучати приватний сектор до вирішення питань кібербезпеки через державно-приватні партнерства. Це дозволить ефективніше використовувати наявні ресурси та експертний потенціал. Успіх міжнародної співпраці України в сфері кібербезпеки залежить від створення довгострокової стратегії, яка враховуватиме: зростання складності кіберзагроз, потребу в постійному навчанні та розвитку експертного потенціалу, адаптацію до швидких технологічних змін у глобальному масштабі.

Ефективна міжнародна співпраця вимагає координації між державними органами, міжнародними партнерами, приватним сектором та громадянським суспільством. Лише інтегрований підхід дозволить Україні забезпечити надійний захист у кіберпросторі. Міжнародна співпраця України у сфері кібербезпеки є важливою умовою для зміцнення національної стійкості до кіберзагроз. Хоча виклики залишаються значними, стратегічний підхід, що включає гармонізацію законодавства, кібердипломатію, інновації та партнерство з ключовими міжнародними гравцями, дозволить Україні посилити свої позиції у глобальній системі кіберзахисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Будапештська конвенція про кіберзлочинність – офіційний міжнародний документ, що регламентує засади боротьби з кіберзлочинами, 2000.

2. Василенко, М. В. «Міжнародне співробітництво України у сфері кібербезпеки».Науковий журнал з проблем безпеки, №3, 2021. с. 45–58.

3. Гармаш, О. П. «Гармонізація законодавства України з міжнародними стандартами кібербезпеки».Київ: Інститут права [2021].

4. Національна стратегія кібербезпеки України на 2021-2025 роки.Доступно на офіційному сайті РНБО України.

5. Денисенко, С. В. «Кібердипломатія як інструмент міжнародного співробітництва України».Журнал міжнародних відносин, №4, 2020. с. 72–84.

6. НАТО і кібербезпека: Розширення співпраці з партнерами.Аналітичний звіт. Офіційний сайт НАТО.2021.

7. Європейський Союз/ «Цифровий порядок денний ЄС: стратегія кібербезпеки».Брюссель: Офіційні документи ЄС. Доступний онлайн, 2016.

8. Ковальчук, І. А. (2021). «Системний підхід до захисту критичної інфраструктури в Україні».Звіт Microsoft про кіберзагрози 2022 року.

9. Аналітичний документ корпорації Microsoft. Доступний онлайн.

10. Міжнародний союз електрозв'язку (ITU). (2020). «Глобальний індекс кібербезпеки».Женева: ITU. Доступний онлайн.

11. Центр кібербезпеки при НАТО: аналіз і рекомендації для партнерів. (2021). Брюссель: Центр передових технологій кібербезпеки. Доступно на сайті.

12. Петренко, О. С. (2023). «Інновації в міжнародній співпраці у сфері кібербезпеки».Монографія. Київ: Наукове видавництво.

13. Шевченко, Л. М. (2021). «Міжнародне право і виклики кіберзлочинності». Журнал юридичних досліджень, №2, с. 14–22.

14. Глобальний форум кібербезпеки (2022). Звіт про заходи.Офіційний сайт форуму.

15. Бойко, Т. І. (2022). «Державно-приватне партнерство у сфері кібербезпеки».Економічна безпека, №5, с. 91–103.

16. ОБСЄ і кібербезпека: Ініціативи для Східної Європи. (2020). Віденський звіт. Офіційний сайт ОБСЄ.

17. Закон України «Про основні засади забезпечення кібербезпеки» (2017). Доступно на сайті Верховної Ради України.

18. Кірєєв, О. В. (2021). «Міжнародний досвід боротьби з кіберзлочинністю та його застосування в Україні».Сучасні проблеми права, №3, с. 36–49.

19. Агенція кібербезпеки ЄС (ENISA). (2021). «Стратегія кіберстійкості для партнерів»Афіни: ENISA. Доступний онлайн.

20. Лебідь, Ю. П. (2023). «Майбутнє кібербезпеки України: перспективи міжнародної співпраці».Аналітичний огляд. Харків: Національний університет.

21. Гринів, С. І. (2020). *Інтеграція України в європейський безпековий простір: політичні та правові аспекти*. Київ: НАН України.

22. Мартиненко, А. В. (2018). *Сучасні виклики безпеки Європи та роль України у їх подоланні*. Львів: Львівський національний університет.

23. Пархомчук, О. І. (2021). *Європейська політика безпеки і оборони: стратегічні виклики для України*. Харків: Видавничий дім «Інтернаука».

24. Ковальчук, О. В. (2020). «Політика Європейського Союзу у сфері безпеки та її вплив на інтеграцію України». *Вісник міжнародних відносин*, №4, с. 10-17.

25. Європейська Комісія (2023). *Спільна стратегія безпеки ЄС та її імплементація в контексті України*. Брюссель: ЄС.

26. Центр досліджень європейської безпеки (2022). *Безпековий простір ЄС та роль України в сучасних геополітичних викликах*. Аналітичний звіт.

27. Гедікова Н. П. Забезпечення національної безпеки України в сучасних умовах євроінтеграційних процесів. В: Соціально-гуманітарні пріоритети України в контексті євроінтеграційних процесів. Одеса, 16 листопада 2017 р.

Ред. кол.: С. В. Албул, Т. І. Койчева, Е. І. Мартинюк та ін. Одеса: Астропринт, 2017. С. 29–31.

28. Гедікова Н. П. Пріоритетні і стратегічні завдання сучасної української геостратегії. В: Сучасна українська держава: вектори розвитку та шляхи мобілізації ресурсів. ІІ Всеукраїнська науково-практична конференція. Одеса, 10 лютого 2017 р. Одеса: ДЗ Південноукраїнський національний педагогічний університет імені К. Д. Ушинського, Центр соціально-політичних досліджень «Politicus», 2017. С. 7–9.

29. Гібридні загрози Україні і суспільна безпека. Досвід ЄС і Східного партнерства. Аналітичний документ. Київ, 2018. 105 с.

30. Горбулін В.П. Засади національної безпеки України: Підручник. Київ: Інтертехнологія, 2009. 272 с.

31. Горбулін В.П. Стратегічне планування: вирішення проблем національної безпеки. Монографія. В.П. Горбулін, А.Б. Качинський. Київ: НІСД, 2010. 288 с.

32. Дзьобань О. П. Проблеми захисту національних інтересів України у сфері державної безпеки в умовах геополітичних трансформацій XXI століття: монографія. Харків: Право, 2013. 295 с.

33. Костенко Г.Ф. Теоретичні аспекти стратегії національної безпеки: Навч. посіб. Київ: ЗАТ Видавничий дім «ДЕМІД», 2002. 144 с.

34. Васильчишин О., Титор В., Кекіш І. Національна безпека держави: особливості забезпечення у режимі воєнного стану. Економічний аналіз. 2022. Т. 32. № 4. С. 289–297.

35. Часник Д.В. Забезпечення прав людини у сфері національної безпеки в умовах протистояння військовій агресії російської федерації. Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична. 2022. Вип. 34. URL: https://nzlubp.org.ua/index.php/journal/article/download/600/551.

36. Смолянюк В. Ф. Національна безпека України: термінологічний баласт чи державотворча необхідність. Суспільно-політичні процеси: науково-популярне видання. 2017. № 2-3. 110 с.

37. Шевченко М.М., Зозуля О.С., Храпач Г.С., Лепіхов А.В. Російсько-українська війна: особливості реалізації загроз державному суверенітету України та перспективи виходу з війни. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2022. № 2(75). URL: http://znp-cvsd.nuou.org.ua/article/view/266598/262571.

38. Національна безпека держави: філософсько-правовий і соціально-економічний аналіз : монографія / В. Бліхар та ін. Хмельницький : ХУУП ім. Л. Юзькова, 2021. 404 с.

39. Вонсович О. Стан національної безпеки України в сучасній геополітичній ситуації. Політичний менеджмент. 2012. № 1–2. URL: https://ipiend.gov.ua/wp-content/uploads/2018/08/vonsonovych_stan.pdf

40. Bahadir Candan, “Top 5 Critical Iinfrastructure Cyberattacks,” *ANAPAYA*, February 23, 2023, https://www.anapaya.net/blog/top-5-critical-infrastructure-cyberattacks.