МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

ФАКУЛЬТЕТ СОЦІАЛЬНИХ НАУК ТА СОЦІАЛЬНИХ ТЕХНОЛОГІЙ

КАФЕДРА МІЖНАРОДНИХ ВІДНОСИН

КВАЛІФІКАЦІЙНА РОБОТА

освітній ступінь - бакалавр

на тему: **«ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В КОНТЕКСТІ МІЖНАРОДНИХ ВІДНОСИН: КІБЕРБЕЗПЕКА ЯК ОДИН ІЗ ВИКЛИКІВ СУЧАСНОЇ ЦИФРОВОЇ ЕПОХИ»**

Виконала:
студентка 4-го року навчання
спеціальності 291 «Міжнародні відносини,
суспільні комунікації та регіональні студії»

Гринчишина Валерія Олександрівна

Науковий керівник:
Гриценко Олена Миколаївна
професор, доктор політичних наук,
професор кафедри міжнародних відносин

КИЇВ 2024

ЗМІСТ

ТЕРМІНОЛОГІЧНИЙ СЛОВНИК ВИЗНАЧЕНЬ І СКОРОЧЕНЬ

ІКТ – інформаційно-комунікаційні технології;

Гіпернет – гіпермедійна інфо-комунікаційна інфраструктура;
НТП – науково-технічний прогрес;

МЦБ – міжнародна цифрова безпека – процес імплементації технічних, політичних, соціально-економічних, юридичних і культурних заходів, що спрямовані на захист держав і світових мереж від кіберзагроз і гарантування стабільності, безпеки та дотримання прав і свобод громадян у міжнародному цифровому середовищі;

Інформаційна безпека – комплекс заходів, спрямованих на захист інформації та засобів її передачі, зберігання, обробки та накопичення;

Цифрова безпека зазвичай пов’язана із захистом мереж, даних і комп’ютерних систем від вторгнення зовнішніх користувачів, застосування вірусів і шкідливого програмного забезпечення;

Кібербезпека полягає в застосуванні стратегій щодо захисту від різного виду загроз і злочинності в кіберпросторі;

Інформаційне суспільство – це нова форма організації суспільства, що виникла на основі інформаційної супермагістралі, що об'єднала різні технології в єдину інтегровану інформаційну систему;

Глобальне інформаційне суспільство – суспільство нового покоління, яке виникає в результаті глобальної соціальної революції, заснованої на стрімкому розвитку інформаційних і телекомунікаційних технологій;
ООН – Організація Об’єднаних Націй;
ОБСЄ – Організація з безпеки і співробітництва в Європі;
ЄС – Європейський Союз;
ЮНЕСКО – Організація Об’єднаних Націй з питань освіти, науки і культури;
МСЕ – Міжнародний Союз Електрозв’язку;

ENISA – Європейське агентство з мережевої та інформаційної безпеки;

UNODA – Офіс Верховного представника ООН з питань роззброєння;

GGE – Група урядових експертів;

ITU – Міжнародний союз електрозв'язку;

CCDCOE – Центр відмінності з кібероборони;

ISO/IEC 27001 – це міжнародний стандарт, який встановлює вимоги до системи управління інформаційною безпекою (ISMS);

SSL/TLS – це криптографічні протоколи, які забезпечують захищене з'єднання між вебсервером і браузером;

HTTPS – розширення протоколу HTTP з використанням SSL/TLS для шифрування даних;

UNGGE – Група урядових експертів ООН з питань інформаційної безпеки;

Національна інформаційна безпека – це багатогранне поняття, яке виходить за рамки забезпечення лише інформаційної безпеки держави, її установ, оборонного та внутрішньополітичного секторів. Доктрина національної інформаційної безпеки враховує захист інтересів індивідів, суспільства та держави. Захист інформаційних інтересів особистості та громадянина є ключовим для визнання держави суб’єктом суспільного договору та носієм суверенітету, що, зі свого боку, є необхідним для захисту прав громадян. Концепція також включає захист інформаційної інфраструктури за допомогою програмних, фізичних і технічних засобів, а також гарантування безпеки наукових досліджень та комерційних секретів;

Стратегія кібербезпеки України – комплексний набір заходів, пріоритетів та напрямів для забезпечення безпеки в кіберпросторі;

РНБО – Рада національної безпеки і оборони України;

CERT-UA – Урядова команда реагування на комп'ютерні надзвичайні події України;

ISACA – Асоціація з аудиту та управління інформаційними системами;

СБУ – Служба безпеки України;

ДССЗЗІ – Державна служба спеціального зв’язку та захисту інформації України;

FIRST – Форум команд реагування на інциденти інформаційної безпеки.

ВСТУП

Актуальність теми дослідження. Сучасна епоха вимагає від людства не лише глибокого розгляду стану міжнародних відносин, а й ґрунтовного аналізу перспектив його майбутнього розвитку. Завдяки новим викликам цивілізаційного поступу сьогодні спостерігається процес кардинального трансформування всесвітнього порядку. Створюється новий соціальний простір, з'являються нові учасники міжнародних відносин, що мають суттєвий вплив на світову політику. Водночас потенціал таких просторів, як технологічний, фінансовий, економічний, розкривається на повну потужність завдяки розширенню інфопростору, стрімкому розвитку інформаційних і комунікативних технологій. Інформатизація стала новим етапом у розвитку продуктивних сил, де обмін інформацією, її оперативна обробка та ефективне використання визначають динаміку розвитку суспільства. Здійснюється перетворення методів виробництва, поглядів споживачів, актуалізується питання міжнародно-правових відносин.

У різних сферах життя все частіше використовуються терміни, пов'язані з інформацією, зокрема, «інформаційні технології», «інформаційні війни», «кіберпростір», «електронний уряд». Сучасну інформаційну революцію пов'язують із виникненням нових інформаційно-комунікаційних технологій на тлі глобалізаційних змін. Нові інформаційно-комунікаційні технології модифікують (зазвичай доповнюють) призначення та функції як державних, так і громадських інститутів, а також різних міжнародних організацій. Тому теоретичний аналіз міжнародних відносин, який ігнорує контекст інформаційно-комунікаційних технологій, уже не може вважатися достатнім для об'єктивного та всебічного розуміння сучасного міжнародного світопорядку. Ці зміни впливають на всі аспекти міжнародних відносин: від процесу ухвалення зовнішньополітичних рішень до розв’язання міжнародних конфліктів. Усвідомлення природи розвитку політичних процесів під впливом інформаційно-комунікаційних технологій (далі ІКТ) є важливою передумовою для ефективного вирішення будь-яких завдань у сфері міжнародних відносин.

Ключовим елементом нових ІКТ є Інтернет, який активно перетворюється на Гіпернет – гіпермедійну інфо-комунікаційну інфраструктуру. Вона визначає становлення нового світу, основними рисами якого є інтернаціоналізація національних економік, універсалізація принципів міжнародної взаємодії в різних галузях, зокрема в економіці, політиці, праві, науці, освіті, культурі та соціальній сфері. Інтернет створив принципово нове середовище для спілкування та взаємодії людей, що робить його особливим об'єктом досліджень вчених у різних галузях науки.

Інформатизація, без сумніву, сприяє більш ефективному управлінню соціально-економічними та соціально-політичними процесами. Проте цей процес не лише прискорює розвиток цивілізації, а й породжує нові загрози для національної, регіональної та глобальної безпеки. Поступова еволюція ІКТ схожа на відкриття «скриньки Пандори», звідки виникають небажані та навіть небезпечні наслідки для суспільства. Стрімкий і непередбачуваний розвиток ІКТ стає новим викликом як для реальної практики соціальних відносин, так і для соціально-політичної теорії. Дослідження питання впливу інформаційно-комунікаційних технологій на сучасні міжнародні відносини та політичні процеси, а також безпека використання ІКТ є актуальним як з теоретичної, так і з практичної точки зору.

Мета дослідження: встановити взаємодію інформаційних технологій і міжнародних відносин, зосереджуючись на проблемі кібербезпеки як одному з ключових викликів сучасної цифрової епохи. Робота визначає теоретико-методологічні засади міжнародної безпеки та глобального інформаційного суспільства, а також виокремлює принципи правового регулювання міжнародних інформаційних відносин.

Поставлена мета дослідження передбачає виконання наступних дослідницьких завдань:

- розглянути становлення та розвиток концепції глобального інформаційного суспільства;
- визначити підходи до термінології та визначення понять у міжнародних безпекових студіях;

- окреслити принципи правового регулювання міжнародних інформаційних відносин;
- встановити особливості розвитку міжнародної архітектури кібербезпеки;
- з’ясувати вплив кіберзагроз на міжнародні відносини та національну безпеку;
- охарактеризувати міжнародну співпрацю в галузі кібербезпеки;
- виокремити участь України в міжнародних ініціативах з кібербезпеки.

Огляд літератури. Дослідження проблеми формування мережевої архітектури публічного управління та системи забезпечення інформаційної безпеки держави, які викладені в працях науковців (Костенко, 2021) та (Левченко, 2021), виявилися ключовими джерелами інформації для дослідження. Процес формування мережевої архітектури та гарантування інформаційної безпеки в контексті національної безпеки, як розглядають ці автори, став основою для аналізу впровадження сучасних технологій у галузі кібербезпеки в Україні. Окрім того, праця Давиденка, О. (2021) щодо державного управління системою профілактики та протидії загрозам суспільно-політичній стабільності України здобула визнання як цінний теоретичний внесок у розуміння проблем сучасної національної безпеки та протидії загрозам. Також погляди Шахової, О. (2018) на роль інформаційних технологій у розвитку міжнародних відносин визначили позицію в роздумах щодо використання сучасних технологій у глобальному інформаційному середовищі. Ці та інші праці вказаних авторів визначили теоретичне та концептуальне підґрунтя та послужили джерелом для реалізації дослідницьких завдань у сфері кібербезпеки.

Проблема дослідження – вплив швидкого розвитку інформаційних технологій на міжнародні відносини з позиції кібербезпеки та боротьба з викликами, що виникають у контексті сучасної цифрової епохи.

Об'єкт дослідження – інформаційні технології в контексті міжнародних відносин.

Предмет дослідження – кібербезпека як один із викликів сучасної цифрової епохи.

Практичне значення дослідження. Дослідження має безпосереднє практичне значення для розуміння та управління викликами, які виникають у

цифровій епосі. Результати дослідження можуть слугувати підґрунтям для розробки та вдосконалення стратегій кібербезпеки на різних рівнях, враховуючи міжнародний, національний і регіональний. Дослідження дозволяє ідентифікувати ключові виклики, пов'язані з кібербезпекою в міжнародних відносинах, і розробляти рекомендації для політик і дій, спрямованих на зміцнення безпеки в цифровому середовищі. Розуміння впливу кіберзагроз на міжнародні відносини може бути основою для розробки превентивних стратегій та міжнародної співпраці у сфері кібербезпеки.

Теоретичне значення дослідження. Дослідження робить важливий внесок у розуміння теоретико-методологічних аспектів міжнародних інформаційних відносин та кібербезпеки. Воно висвітлює різноманітні підходи до термінології та визначення понять у міжнародних безпекових студіях, а також допомагає врівноважити концепції глобального інформаційного суспільства та принципи правового регулювання міжнародних інформаційних відносин. Його теоретичний внесок полягає у виокремленні зв’язків між інформаційними технологіями та міжнародною безпекою, сприяючи розвитку та вдосконаленню теорії в цій області.

Методи дослідження. Під час здійснення дослідження використовувалися метод системного підходу для вивчення та узагальнення чинних теоретичних концепцій, а також метод історичного аналізу для вивчення еволюції понять і принципів правового регулювання міжнародних інформаційних відносин.

Переважним у роботі є метод системного аналізу, що дозволив комплексно проаналізувати проблеми розвитку інформаційної політики та кібербезпеки, зокрема, правові аспекти, міжнародні стандарти та оцінку глобальних загроз у контексті швидкої трансформації інфопростору. Під час дослідження було проаналізовано правове регулювання безпеки в інформаційній сфері, зокрема, гармонізація національних законів, приватність і захист даних, відсутність єдиного міжнародного стандарту в правовому регулюванні інформаційних відносин тощо. Окрім цього, були досліджені чинники, що ускладнюють міжнародну співпрацю в контексті гарантування безпеки в інфопросторі, зокрема, розбіжність у політичних аспектах, а також економічні та технологічні різниці потенціалів різних держав.

Завдяки системному підходу вдалося розглянути виклики інформаційної безпеки як частину більшої системи, а отже, врахувати всі її складові та взаємозв'язки між ними. Зокрема, вдалося уникнути ізольованого підходу, що означає не зосередження на окремих факторах, яке може призвести до неповного розуміння суті проблеми, а дослідження різноманітних аспектів системи: економічних, соціальних, політичних.

Окрім того, використання методу історичного аналізу дозволило прослідкувати еволюцію понять, дослідити становлення та розвиток глобального інформаційного суспільства, а також дало розуміння перспектив правового регулювання міжнародних інформаційних відносин.

Завдяки використанню методу історичного аналізу вдалося застосувати напрацювання таких науковців, як Мануель Кастельс з його визначенням інформаціоналізму, О. Шахова та її концепцію інформаційного суспільства, а також Жак Еллюль з його працею "Інша революція" та концепцією інформаційно-технічної цивілізації.

Структура дослідження. Робота складається з термінологічного словника визначень і скорочень, вступу, трьох розділів, висновків, списку використаних джерел, анотації та додатків.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ

1.1. Сучасні підходи до вивчення термінології та визначення понять у міжнародних безпекових студіях

Науково-технічний прогрес, який далі буде позначений як НТП, представляє собою досягнення людства та необхідну умову для досягнення прогресу та демократизації. Однак продукти цього прогресу також стали джерелом нових загроз і викликів для міжнародного миру, стабільності та безпеки. Серед таких загроз важливе місце посідає використання інформаційно-комунікаційних технологій (далі – ІКТ), які, коли використовуються з неправильними цілями, призводять до виникнення інформаційної зброї, злочинної діяльності та інформаційних воєн. Інформаційний простір стає значущим етапом у розвитку ІКТ та відрізняється від традиційних міжнародних просторів, таких як повітряний, морський, та земельний (Піпченко, Макаренко, Рижков, 2019).

Міжнародна цифрова безпека (далі – МЦБ) – це процес імплементації технічних, політичних, соціально-економічних, юридичних і культурних заходів, що спрямовані на захист держав і світових мереж від кіберзагроз і гарантування стабільності, безпеки та дотримання прав і свобод громадян у міжнародному цифровому середовищі. Феномен МЦБ є складним процесом, що вимагає вивчення суміжних термінів, таких як інформаційний простір та інформаційне суспільство, для його кращого розуміння. Деякі фахівці акцентують увагу на важливій різниці між цими термінами, які часто використовуються як синоніми. Інформаційний простір охоплює сукупність інформаційних ресурсів, систем і технологій, що працюють на загальних принципах та структурують взаємодію між людьми. До нього належать неживі об’єкти та результати інформаційної діяльності людства. Якщо говорити про інформаційне суспільство, також відоме як розумне суспільство, то воно представляє собою нову фазу розвитку цивілізації, у якій ключовими

продуктами є інформація та оцифровані знання, а головним елементом – людина (Закіров, 2017).

У період екстремально швидкого розвитку науки та широкого впровадження високих технологій у повсякденне життя, що призвело до загальної комп'ютеризації, інтегрованість в інформаційний простір стає визначальним чинником для ключових напрямів прогресу. Сама інформація стає важливим стратегічним ресурсом сучасної держави. Інформаційний простір віддзеркалює поточну політичну карту світу та всі важливі тенденції, а процес інформатизації охоплює всіх учасників світової політики – від приватних осіб до провідних міжнародних організацій.

Поняття інформаційної безпеки в сучасній науковій літературі визначається неоднозначно. Можна виділити три фундаментально різні підходи до трактування його змісту. У першому випадку, інформаційна безпека розглядається як комплекс заходів, спрямованих на захист інформації та засобів її передачі, зберігання, обробки та накопичення. У другому випадку, це трактування передбачає захист від різноманітних інформаційних впливів або комплекс заходів для протидії впливу інформаційної війни. У третьому випадку, проблематика інформаційної безпеки охоплює практично всі аспекти життєдіяльності особистості, суспільства та держави, пов'язані з виробництвом, перетворенням, споживанням, накопиченням та зберіганням інформації, незалежно від методів і засобів здійснення цих процесів (це так зване розширювальне тлумачення) (Карпчук, 2018).

Якщо говорити про різні тенденції в тлумаченні інформаційної безпеки серед дослідників, спостерігаються деякі відмінності в розумінні цього поняття. Зокрема, значна увага приділяється гарантуванню безпеки телекомунікаційних та автоматизованих інформаційних систем, а також інформації, що зберігається та обробляється на персональних комп'ютерах (Піпченко, Рижков, 2021). Ця тенденція стає панівною серед дослідників, і вона повністю обґрунтована та викликана низкою факторів, зокрема:

- електронні засоби обробки, передачі, накопичення та зберігання інформації є основою більшості сучасних інформаційних технологій.

- технічні засоби, спрямовані на таємне отримання інформації, набули широкого поширення і на початковому етапі не зазнали належної протидії.
- правові аспекти щодо інформаційної безпеки мають суперечливий та недосконалий характер.
- недостатня кількість фахівців гуманітарного профілю (особливо юристів) у цій галузі.
- недостатність комплексних розробок з питань гарантування інформаційної безпеки, які би включали в себе експертів з гуманітарних і технічних галузей.

На думку Боднар (2016), поняття кібербезпеки охоплює множину проблем різного характеру і включає ще більше рішень. Кібербезпека є питанням активних досліджень і розробок у галузі інформаційних технологій з урахуванням усіх складових екосистеми ІКТ. Схематично поняття «кібербезпека» представлено на рис. 1.1

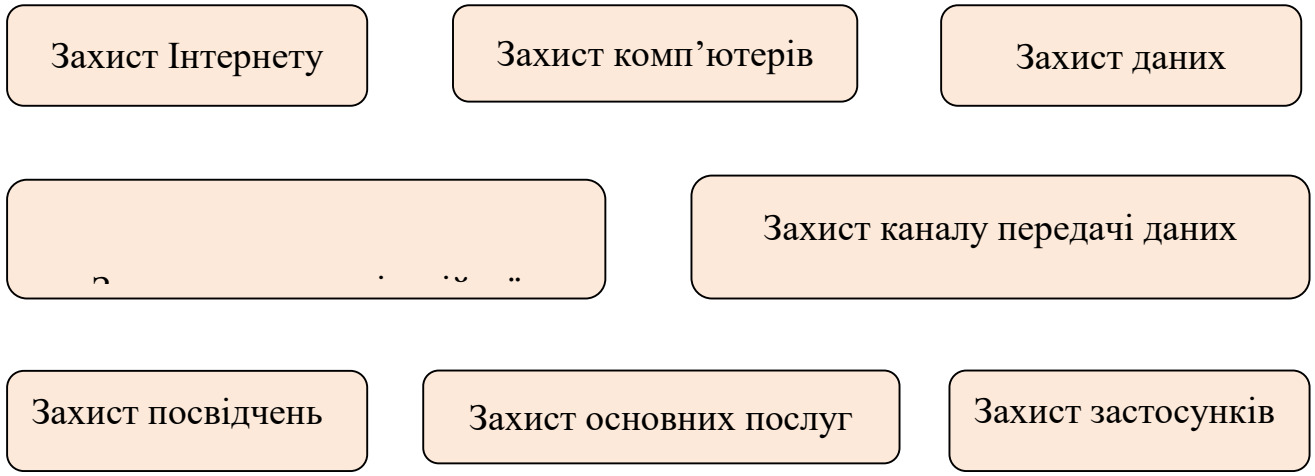

Рис.1.1 Теми та напрями кібербезпеки

Говорячи про спільність і відмінність між поняттями міжнародної цифрової безпеки (МЦБ), інформаційної безпеки та кібербезпеки, слід зауважити, що цифрова безпека зазвичай пов’язана із захистом мереж, даних і комп’ютерних систем від вторгнення зовнішніх користувачів, застосування вірусів і шкідливого програмного

забезпечення. Інформаційна безпека, з іншого боку, пов’язана із захистом будь-якого виду інформації, незалежно від її форми (паперова, цифрова, графічна, звукова тощо). Щодо кібербезпеки, то зазвичай її ототожнюють із цифровою безпекою, адже перша так само полягає в застосуванні стратегій щодо захисту від різного виду загроз і злочинності в кіберпросторі. Проте цифрова безпека може охоплювати більший набір заходів щодо забезпечення захисту цифрового середовища: гарантування безпеки під час виникнення технічних недоліків, людського фактору та/або інших непередбачуваних обставин. Безперечно, усі ці поняття переплітаються, а два останні можуть використовуватися взаємозамінно, проте кожне з них охоплює різні аспекти захисту технологічних ресурсів і цифрових систем.

Забезпечення захисту комп'ютерів (серверів, настільних комп'ютерів, ноутбуків чи смартфонів) є метою роботи різноманітних груп у межах ІТ- та Інтернет-спільноти. Кібербезпека все частіше розглядається як стратегічна проблема держави, яка комплексно впливає на економіку країни. Це включає взаємодію національних розробників програмного забезпечення та систем управління, виробників обладнання та компонентів для забезпечення ІКТ-інфраструктури (Варламова, Дем’янова, 2020). Низька ринкова конкурентоспроможність цих суб'єктів призводить до потреби використання рішень від іноземних виробників.

На практиці це явище призводить до стрімкого зростання залежності від іноземних виробників і зниження рівня інформаційного захисту через примусове використання «закритого» програмного та апаратного забезпечення у всіх сегментах інфраструктури, як для спеціальних державних відомств, так і для цивільного сектору. З часом, залежність від іноземних виробників обладнання та розробників програмного забезпечення може досягти критичного рівня (Воронкова, 2017).

На думку Воронкової (2017), підприємства-розробники та виробники повинні приділяти особливу увагу питанням інформаційної безпеки в продукції, яку вони розробляють або випускають. Це передбачає високі вимоги до надійності та захищеності запропонованих рішень. Тільки в крайніх випадках, і тільки за необхідності підвищення ринкової орієнтованості окремих продуктів, варто

використовувати рішення іноземних вендорів і розробників програмного забезпечення.

1.2. Концепція глобального інформаційного суспільства: становлення та розвиток

Інформаційне суспільство – це нова форма організації суспільства, що виникла на основі інформаційної супермагістралі, що об'єднала різні технології в єдину інтегровану інформаційну систему. Зростання важливості інтелектуальних послуг у фінансовій сфері та інші технічно-економічні трансформації стали основою для формування сучасної держави. Мануель Кастельс у своєму творі «Інформаційний вік: економіка, суспільство і культура» (1999) визначає риси інформаційної економіки, що характеризують її як сучасний тип економіки, де основним аспектом є перетворення інформації на один із ключових факторів соціально-економічного прогресу, що впливає як на суспільство в цілому, так і на окремого індивіда.

За Кастельсом (1999), суспільство інформаціоналізму тісно взаємодіє з процесами глобалізації. Автор вивчає умови народження нового інформаційного суспільства, культури й економіки, що виникли в США після революції в інформаційних технологіях, таких як телебачення та комп’ютери, що спричинили фундаментальні зміни в капіталістичній системі з 1980-х років і призвели до формування «інформаційного капіталізму». «Інформаційні суспільства» базуються на інформаціоналізмі (Таблиця 1.1) – розвитку, у якому якісна здатність оптимізувати використання факторів виробництва на основі знань та інформації є основним джерелом продуктивності.

Таблиця 1.1

Основні риси інформаційної економіки за концепцією «інформаціоналізму» М. Кастельса

№	Показник	Характеристика
1	Інформація як основний ресурс економіки	Інформація розглядається як основна «сировина» економіки, що визначає її функціональність і розвиток.
2	Вплив інформаційної технології на суспільство та людину	Інформаційна технологія глибоко впливає на суспільство та індивіда, визначаючи їхні можливості та перспективи.
3	Рівень обробки інформації та застосування мережевої логіки	Інформаційні технології дозволяють застосовувати мережеву логіку до економічних процесів та організацій на високому рівні оброблення інформації.
4	Гнучкість завдяки технології та мережевій логіці	Інформаційна технологія та мережева логіка забезпечують гнучкість, що дозволяє легко змінювати процеси, організації та інститути при виникненні нових форм.
5	Інтеграція індивідуальних технологій	Різні індивідуальні технології зливаються в єдину інтегровану систему, що посилює їхню ефективність та взаємодію.

У 1980-і роки виникла нова глобальна інформаційна економіка, яка виявила неабияку прибутковість. Вона визначається як інформаційна, оскільки продуктивність і конкурентоспроможність її економічних суб'єктів (фірми, регіони чи держава) суттєво залежать від їхньої здатності генерувати, обробляти та ефективно використовувати інформацію, що базується на знаннях. Ця економіка є глобальною, оскільки вона має можливість функціонувати як єдина система в реальному часі на всій планеті (Makedon, Drobyazko, Shevtsova, Maslosh, Kasatkina, 2019).

Нова «інформаційна» економіка відрізняється від просто інформаційної тим, що культурно-інституціональні властивості всієї політичної та соціальної системи впливають на поширення та функціонування цієї нової економіки. Це сприяє виникненню нової форми інформаційного підприємства, яке характеризується гнучким (не масовим) виробництвом, інноваційними системами управління, організаційною структурою, що ґрунтується на горизонтальній, а не вертикальній моделі, і об'єднанням великих корпорацій у стратегічні альянси (Висоцький, 2017).

Концепція глобального інформаційного суспільства несе ідеологічний зміст, її формування пов'язане з конкретним політичним, юридичним і економічним устроєм (Гуйван, 2018). Реалізація концепції інформаційного суспільства виступає каталізатором глибших і масштабніших трансформацій у світі, що виходять за межі лише технологічного прогресу та всеосяжного впровадження ІКТ. Перехід від виробництва матеріальних до інформаційних продуктів визначає ключову роль освіченості та розвитку суспільства.

Так, із середини XX століття визначальним фактором соціально-економічного розвитку стає перехід від «економіки речей» до «економіки знань», що супроводжується значним посиленням ролі інформації у вирішенні практично всіх завдань світової спільноти. Це свідчить про те, що науково-технічна революція поступово перетворюється на інтелектуально-інформаційну. Інформація стає не лише об'єктом спілкування, а й прибутковим товаром, ефективним сучасним інструментом організації та управління суспільним виробництвом, наукою, культурою, освітою та соціально-економічним розвитком суспільства в цілому (Лісовський, 2017).

Актуальні концепції, які сприяли народженню інформаційного суспільства, включають такі ідеї:

- зміна технотронної цивілізації на антропогенну, за твердженням Г. Ділігенського.
- початок постісторичного періоду, визначений Ф. Фукуямою як «кінець історії».

- народження «багатовимірної людини» в постіндустріальній цивілізації за концепцією Г. Маркузе.

У концепції інформаційного суспільства, яке вважається цивілізаційною парадигмою сучасного розвитку, відображаються такі основні аспекти:

- з'являється домінування «четвертої» інформаційної сфери економіки, що слідує за сільським господарством, промисловістю та економікою послуг.
- значно зростає інтелектуалізація праці, відзначаючи підвищення ролі інтелектуальних здібностей у виробництві та робочому процесі.
- відбуваються якісні зміни у всіх сферах громадського життя, визначаючи новий характер їх функціонування та взаємодії (Шахова, 2018).

Інформаційний тип суспільства був сформований завдяки інформаційно-комунікативному прогресу соціуму, який представляє собою цивілізаційну парадигму XXI століття. Інформаційне суспільство розглядається як варіант постіндустріального суспільства. Його концепція ґрунтується на тому, що інформаційний сектор у високорозвинених країнах починає значно випереджати традиційні галузі за темпами зростання, і очікується, що ця тенденція посилиться в майбутньому (Еллюль, 1999).

Загальні підходи дають можливість визначити «глобальне інформаційне суспільство» як:

- суспільство нового покоління, яке виникає в результаті глобальної соціальної революції, заснованої на стрімкому розвитку ІКТ;
- знання-орієнтоване суспільство, де ключовою умовою добробуту кожної людини і держави є знання, набуте завдяки вільному доступу до інформації та навичкам роботи з нею;
- глобальне суспільство, де обмін інформацією не знає часових, просторових або політичних обмежень, де наукова обробка даних і підтримка знань сприяють ухваленню обґрунтованих рішень для покращення якості життя в усіх аспектах;
- суспільство, що сприяє взаємопроникненню культур та відкриває нові можливості для самореалізації кожного співтовариства (Литвин, 2020).

Так, інформація стає ключовим природним ресурсом для розвитку цивілізаційної парадигми, визначаючи швидкість і напрями інформаційних переваг. Розвиток людства стає результатом обробки інформації. Інформація зростає в значущості як інструмент праці, виступаючи одним із ключових структурних компонентів сучасної інформаційної цивілізації XXI століття.

1.3. Принципи правового регулювання міжнародних інформаційних відносин: проблеми впровадження

Зростання обсягу обміну інформацією між країнами вимагає чіткого та ефективного правового регулювання для гарантування безпеки, конфіденційності та взаєморозуміння. Принципи правового регулювання міжнародних інформаційних відносин стають ключовим фактором у розв’язанні проблем, що виникають у зв'язку з дедалі більшою комплексністю та динамікою цієї сфери.

Міжнародне право визначає, що забезпечення об’єктивної інформації є ключовою умовою ефективної реалізації всіх інших прав і свобод громадян. Орієнтація на конституційні положення про недоторканність приватного життя та конфіденційність кореспонденції є основою для розробки всієї системи нормативно-правового забезпечення безпеки в інформаційній сфері, оскільки права та свободи індивіда мають найвищий пріоритет. Концептуальні принципи та засади щодо правового регулювання безпеки в інформаційній сфері, розроблені на міжнародному рівні, у відповідності з пунктом 49 Резолюції 2200A (XXI) Генеральної Асамблеї ООН, у різних ступенях відображаються в законодавстві економічно розвинених країн, відзначає комісія Європейського Союзу з кібербезпеки (Стройко, 2018).

Основним стратегічним завданням гарантування інформаційної безпеки є збереження стійкості інформаційного простору, уникнення порушень прав особистості, суспільства й держави. Конституційно-правова база повинна створювати основи для впровадження політики інформаційної безпеки для всіх

трьох суб'єктів – держави, суспільства та особистості, з урахуванням специфічних вимог кожного об'єкта до захисту своїх ресурсів.

Експоненціальний розвиток інформаційно-комунікаційних технологій становить виклик для національної безпеки, оскільки впливає на захист інтересів особистості, суспільства та держави в інформаційній сфері. Неконтрольовані процеси в глобальних мережах та особливості політичної боротьби у віртуальному просторі безпосередньо та опосередковано впливають на забезпечення захисту національних інтересів. Цей виклик національної безпеки стає надзвичайно актуальним через створення відкритих інформаційних мереж та їх з'єднання з міжнародними телекомунікаційними мережами. Свідченням загрози національній безпеці є факт того, що розробка віртуальної міжнародної мережі та вдосконалення технологій контролю активно координується Міністерством оборони США (Еннан, 2020).

Впровадження принципів правового регулювання міжнародних інформаційних відносин стикається з низкою викликів і перешкод, що вимагають уважного розгляду для забезпечення ефективності та стабільності в цій сфері.

Гармонізація національних законів. Різниця в правових системах різних країн є важливим фактором, який ускладнює розробку та впровадження єдиної міжнародної системи правового регулювання міжнародних інформаційних відносин. Законодавство кожної країни формується на основі унікальних правових традицій, культурних особливостей і соціальних потреб. Ця різноманітність створює прогалини та конфлікти в правових стандартах, що можуть ускладнювати ефективність міжнародного співробітництва у сфері інформаційної безпеки. Для уникнення непорозумінь і створення єдиної міжнародної системи правового регулювання, необхідно досягти гармонізації національних законів. Це передбачає вирівнювання та узгодження правових стандартів між державами для створення спільної правової основи, яка враховує специфіку міжнародних інформаційних відносин (White, 2016).

Приватність і захист даних. Сучасна інформаційна дійсність характеризується нестримним зростанням обсягів обміну інформацією на

глобальному рівні. Велика кількість особистих даних перетинає кордони, що вимагає вдосконалення заходів з їх захисту. Приватність визначається як основоположний принцип, що визнає право кожної особи на захист свого особистого життя та конфіденційності. Забезпечення високого рівня захисту приватності та особистих даних є важливою передумовою для підтримки довіри та сприяння стабільності в міжнародних інформаційних відносинах.

Кібербезпека. Сучасний кіберпростір став ареною щоразу більшої кількості кіберзагроз і кібератак, що ставить під загрозу як інформаційні системи, так і державну безпеку. Гарантування кібербезпеки стає важливим аспектом для збереження стабільності та довіри в міжнародних відносинах. Спільні зусилля у сфері кібербезпеки, наприклад, розробка ефективних міжнародних стандартів і механізмів захисту допомагають забезпечити стабільність інформаційних систем та держбезпеки, що є ключовим для уникнення потенційних загроз та викликів у міжнародних відносинах (White, 2016).

Відсутність єдиного стандарту. Відсутність єдиного міжнародного стандарту в правовому регулюванні інформаційних відносин стає важливим фактором, що породжує непорозуміння та труднощі у взаємодії між державами. Нині, при стрімкому розвитку глобальних інформаційних технологій, відсутність єдиної нормативної бази стає викликом для встановлення єдиної правової системи, яка задовольняла би різноманітні інтереси та потреби країн. Це створює простір для різних інтерпретацій та впровадження національних правових підходів, що призводить до нормативних розбіжностей, що може провокувати конфлікти в інформаційних відносинах та обмежувати можливості ефективної співпраці між країнами (Kaufmann, Jeandesboz, 2017).

Забезпечення високого рівня довіри між державами та сприяння міжнародній співпраці вимагає подолання низки складнощів, що виникають через політичні, економічні та культурні розбіжності між національними суб'єктами. Розбіжності в політичних поглядах, інтересах і стратегіях держав можуть негативно впливати на створення спільних нормативів і механізмів, необхідних для забезпечення контролю над кіберзагрозами та іншими аспектами безпеки. Економічні та технологічні

різниці між країнами можуть впливати на рівень готовності до обміну інформацією в контексті кібербезпеки. Зокрема, різноманітні культурні контексти можуть призводити до відмінностей у підходах до розуміння та подолання завдань у сфері інформаційної безпеки. Налагодження співпраці вимагає врахування і культурних особливостей, що можуть впливати на сприйняття безпекових заходів. Умови взаємодії повинні враховувати всі ці розходження для ефективної реалізації спільних стратегій (Стройко, 2018).

Висновок до першого розділу

1. Існують три принципово різні підходи до трактування інформаційної безпеки. Перший підхід розглядає це поняття як комплекс заходів, спрямованих на захист інформації та засобів її обробки та передачі. Другий підхід вбачає інформаційну безпеку як захист від інформаційних впливів різного роду та включає в себе стратегії протидії інформаційній війні. Третій підхід розширює сферу дослідження на всі сфери життєдіяльності особистості, суспільства та держави, пов'язані з обробкою інформації, незалежно від методів та засобів здійснення цих процесів. Цей аналіз підкреслив важливість розуміння та врахування різноманітності підходів до термінології в галузі інформаційної безпеки, оскільки це може визначити ефективність стратегій і заходів з кібербезпеки в міжнародному контексті.

2. Концепція глобального інформаційного суспільства визначає нову еру, де інформаційні технології стають визначальним чинником розвитку. Становлення та розвиток цієї концепції свідчать про перехід до нових цивілізаційних парадигм, де інформація є ключовим ресурсом. Інформаційний сектор у високорозвинених країнах починає значно випереджати традиційні галузі за темпами зростання, і очікується, що ця тенденція посилиться в майбутньому. Перехід від виробництва матеріальних до інформаційних продуктів визначає ключову роль освіченості та розвитку суспільства.

3. Орієнтація на конституційні положення про недоторканність приватного життя є основою для нормативно-правового забезпечення безпеки в інформаційній сфері, оскільки права та свободи індивіда мають найвищий пріоритет. Проблеми впровадження принципів правового регулювання міжнародних інформаційних відносин визначаються відсутністю єдиного стандарту, що ускладнює створення єдиної міжнародної системи правового регулювання. Гармонізація національних законів, вирішення питань приватності та кібербезпеки, а також встановлення довіри та міжнародної співпраці вимагають консолідованих зусиль для забезпечення стабільності та ефективності в інформаційному просторі.

РОЗДІЛ 2
КІБЕРБЕЗПЕКА В КОНТЕКСТІ МІЖНАРОДНИХ ВІДНОСИН

2.1. Міжнародна співпраця в галузі кібербезпеки

Міжнародна співпраця в галузі кібербезпеки є ключовим елементом забезпечення стійкості та безпеки глобального інформаційного простору. У відповідь на зростання кіберзагроз, що не знають національних кордонів, держави, міжнародні організації, приватний сектор і громадянське суспільство активізували свої зусилля для розробки ефективних механізмів взаємодії.

Організація Об'єднаних Націй, Європейський Союз, ОБСЄ та інші міжнародні інституції відіграють важливу роль у формуванні базових принципів та норм, спрямованих на зміцнення кібербезпеки. Вони виступають ініціаторами ухвалення міжнародних конвенцій, створення регулятивних рамок і рекомендацій, що сприяють підвищенню рівня захисту кіберпростору (Антонюк, 2021). Це особливо важливо, оскільки міжнародні організації були створені для консолідованих зусиль держав у досягненні спільних цілей. Однак, у зв'язку з динамікою міжнародних відносин, ці цілі можуть еволюціонувати, вимагаючи відповідних змін у політиці та стратегії міжнародних організацій (Давиденко, 2021).

Міжнародні організації, які не адаптуються до сучасних викликів, стають менш авторитетними, у той час як ті, що гнучко адаптують свою діяльність до новітніх вимог, збільшують свій вплив. Цей процес формує новий ландшафт на міжнародній арені, де різні суб'єкти світової політики можуть виявитися ефективними платформами для вирішення актуальних проблем сучасності. Згідно з думкою Левченко (2021), щоразу більші виклики безпеки вимагають нових форм міжнародного співробітництва на основі міжнародного права. В умовах XXI століття МЦБ повинна стати всебічною та об'єднати всі держави та регіони, враховуючи всі фактори, що впливають на міжнародну систему.

У сучасних умовах ситуація щодо майбутнього глобального кіберпростору перебуває на перетині двох ключових тенденцій. З одного боку, офіційні зусилля світової спільноти спрямовані на демілітаризацію кіберпростору та запобігання його перетворенню на нову арену збройних конфліктів. З іншого боку, міжнародні організації, такі як ООН, хоч і намагаються впливати на цей процес, проте їхні зусилля є досить розфрагментованими.

ООН активно залучена в заходи, пов'язані з безпекою, зокрема у сфері інформаційної безпеки. Її зусилля зосереджені на створенні міжнародної правової основи та розробці політичних документів, спрямованих на боротьбу з незаконним використанням досягнень НТП терористичними групами та організованою злочинністю.

У період з 1998 по 2015 роки питання міжнародної інформаційної безпеки було систематично розглянуте на Генеральній Асамблеї ООН з метою розробки відповідного міжнародного документа. Резолюції «Роль науки і техніки в контексті міжнародної безпеки і роззброєння» та «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки» містили положення про використання високих технологій як у цивільній, так і у воєнній сферах, роль науки й техніки в модернізації озброєнь і важливість протидії деструктивним впливам.

З урахуванням поширення кіберзагроз, Генеральна Асамблея ООН ухвалила резолюцію «Заохочення відповідальної поведінки держав у кіберпросторі в контексті міжнародної безпеки» у 2019 році. Цей документ підтверджує необхідність створення відкритого, безпечного, стабільного й доступного інформаційно-комунікаційного середовища. Також він закликає до встановлення довірчих відносин між державами, розширення можливостей співпраці та заохочення використання новітніх технологій, спрямованих на зменшення ризику конфліктів (Левченко, 2021).

У структурі ООН було сформовано Групу високого рівня для розгляду загроз, викликів і змін, а також обговорюється ідея призначення єдиного координатора ООН у справах боротьби з тероризмом і створення комісії. Що стосується Європи, то до недавнього часу питання кібербезпеки було вирішено лише обмежено,

зосереджуючись на боротьбі з кіберзлочинністю. Це демонструє прийняття Радою Європи Конвенції про кіберзлочинність у 2001 році.

Чимало документів ООН у галузі кібербезпеки мають неоднозначний характер і не завжди визнаються деякими державами-членами як основоположні. Проте останнім часом спостерігається зростання активності ООН у розробці нормативних регуляцій світової кібербезпеки. Наприклад, у червні 2015 року, після засідання Групи урядових експертів ООН з міжнародної інформаційної безпеки, було визнано, що міжнародне право застосовується до сфери використання ІКТ, але в разі необхідності може бути доповнене, включно із запровадженням нових норм.

З 2019 року дискусії щодо питань кібербезпеки в ООН пережили значні зміни через різке зростання глобальних гібридних загроз на міжнародному рівні. Незважаючи на ухвалення різних рішень та резолюцій, ООН досі не запровадила ефективний міжнародно-правовий механізм, спрямований на оптимізацію проблем кібербезпеки.

З розвитком глобального інформаційного суспільства питання інформаційної безпеки набуло великого значення і для діяльності таких спеціалізованих агенцій ООН, як ЮНЕСКО та Міжнародний Союз Електрозв'язку (МСЕ), які реалізують гуманітарні та технічні ініціативи (Запорожець, 2020). Економічна та соціальна рада ООН надає звіти для створення статистичної інформації про застосування ІКТ у світі та на національних рівнях. ЮНЕСКО, що входить до структури ООН та спеціалізується на освіті, науці та культурі, активно займається утвердженням миру та безпеки через розширення співпраці в галузі освіти, науки та культури. Організація спрямовує свою діяльність у сфері комунікацій на зменшення розриву між розвиненими країнами, та країнами, що розвиваються, забезпечуючи безперешкодний доступ до інформації у всьому світі (Сагайдак, 2017).

У 2004 році Європейський Союз усвідомив важливість кібербезпеки та заснував Європейське агентство з мережевої та інформаційної безпеки. У 2012 році агентство опублікувало доклад «Національні стратегії кібербезпеки: Практичний посібник з розробки та впровадження» (Коваленко, 2022).

У 2013 році ОБСЄ внесла ключові ініціативи, ухваливши рекомендації для підсилення довіри в кіберпросторі, що включали заходи для зростання прозорості й безпеки на регіональному рівні. Ці заходи охоплювали співпрацю з приватним сектором та провайдерами критично важливої інфраструктури, а також розробку спільних стратегій управління кібербезпекою.

НАТО, яка є однією з найбільш впливових та авторитетних міжнародних організацій, активно розвиває свою безпекову політику, особливо в контексті кіберпростору, розглядаючи його як арену протистояння та середовище інформаційної війни, з основним акцентом на кібербезпеці. Альянс підкреслив свій оборонний мандат, визнавши кіберпростір як одне із середовищ, у якому необхідно ефективно захищатися, аналогічно до інших фізичних арен міжнародних конфліктів. Командування НАТО зі швидкого реагування на кіберзагрози взяло на себе зобов'язання допомагати союзникам у протидії кібератакам, включаючи можливість використання національних підрозділів кібербезпеки для спеціальних операцій задля захисту держав-членів.

У 2019 році НАТО ухвалила рекомендації, що містять низку інструментів для наступних цілей:

- посилення спроможностей для ефективного реагування на кібератаки, щоб відповісти на дедалі вищу загрозу в кіберпросторі.
- активізація співпраці з діловими партнерами та бізнес-середовищем у розвитку кіберпромисловості, щоб забезпечити спільні зусилля в зміцненні кібербезпеки.
- розвиток можливостей використання кіберпростору союзниками на основі рекомендаційних та безпечних норм, щоб гарантувати безпеку та ефективність діяльності в мережі (Vevera, 2018).

Так, міжнародна співпраця в галузі кібербезпеки вимагає постійної адаптації до нестабільного ландшафту кіберзагроз, що включає розробку єдиних стандартів, принципів регулювання та координації дій на глобальному рівні задля гарантування безпеки та стабільності в кіберпросторі.

2.2. Розвиток міжнародної архітектури кібербезпеки

Архітектура міжнародної інформаційної безпеки – це складна й багаторівнева система, яка включає в себе правові, технічні, організаційні, нормативно-етичні аспекти взаємодії держав, міжнародних організацій, приватного сектору та громадянського суспільства. Її основна мета – забезпечення стабільності глобального інформаційного простору, захист інформації від нелегального доступу, забезпечення конфіденційності, цілісності та доступності даних.

На зламі XX та XXI століття розвиток Інтернету та швидка цифровізація світу відкрили новий етап в історії інформаційної безпеки. Поява Інтернету призвела до значного розширення доступу до інформації, але водночас створила нові загрози, пов'язані з кіберзлочинністю та зловживанням ІКТ.

У 2001 році ґрунтовним кроком у розвитку міжнародної інформаційної безпеки стало підписання Будапештської конвенції про кіберзлочинність. Ця конвенція, прийнята Радою Європи, стала першим міжнародним правовим актом, спрямованим на боротьбу з кіберзлочинністю та забезпечення ефективної співпраці держав у цьому напрямі. Протягом 2000-х років зростала потреба в активній міжнародній співпраці для протидії загрозам кіберпростору. З метою розробки спільних стратегій і стандартів були запущені різні регіональні та глобальні ініціативи: наприклад, у 2005 році США оголосили про стратегію національної кібербезпеки, що покладала акцент на міжнародну співпрацю (Коваленко, 2022).

Загострення потенційної небезпеки обґрунтована можливістю розробки, застосування та розповсюдження інформаційної зброї, загрозою інформаційних війн та інформаційного тероризму, здатних провокувати інформаційні конфлікти зі значними руйнівними наслідками. Тому силами міжнародних співтовариств впроваджується комплекс відповідних заходів з міжнародної інформаційної безпеки, основою якого є міжнародні Договори та Декларації за результатами самітів держав. Водночас в умовах війни росії проти України необхідним є перегляд актуальності та ефективності таких Договорів і Декларацій.

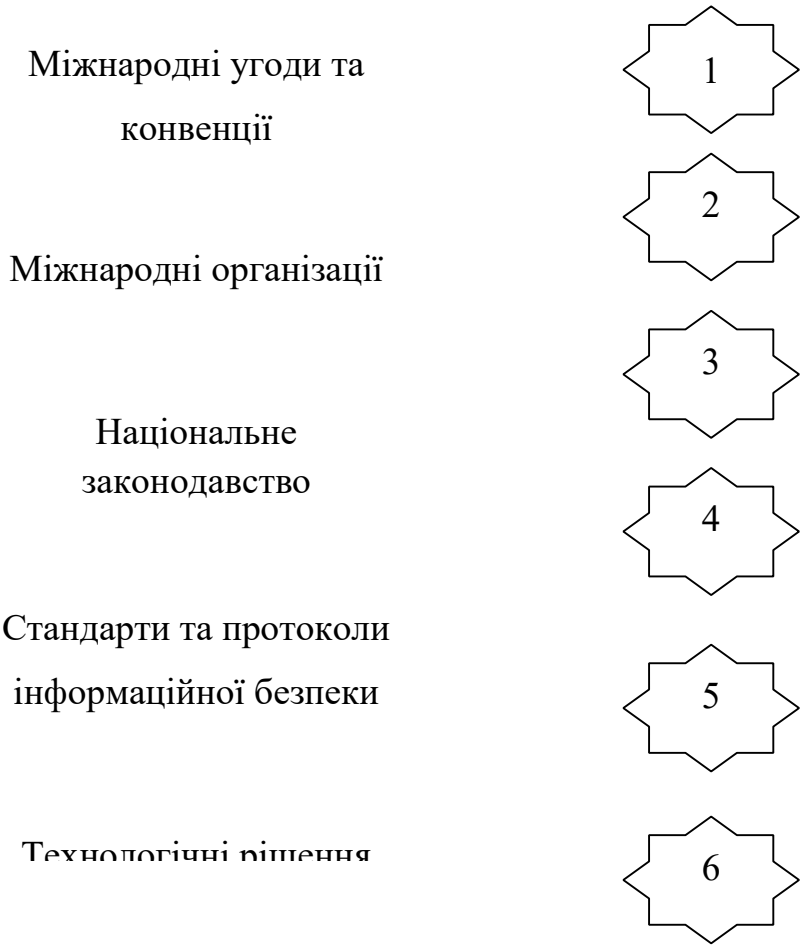

Рис. 2.1 Ключові компоненти архітектури міжнародної інформаційної безпеки

Розгляньмо кожний компонент детально:

1. Міжнародні угоди та конвенції

Міжнародні угоди та конвенції відіграють визначальну роль у формуванні юридичної основи міжнародної інформаційної безпеки. Ці документи розробляються та укладаються міжнародними спільнотами для регулювання питань кібербезпеки та встановлення стандартів, що забезпечують колективну захищеність у кіберпросторі (Коваленко, 2022).

Одним із ключових прикладів такої конвенції, як уже зазначалось вище, є Будапештська конвенція про кіберзлочинність. Ця конвенція, ухвалена під егідою Ради Європи, стала першою міжнародною угодою, що стосується кіберзлочинності та кібербезпеки. У 2019 році Україна ратифікувала Будапештську конвенцію. Після цього, за співпрацею з іншими країнами-учасницями, було розкрито кілька

міжнародних кіберзлочинних груп, що використовували різні види атак на інформаційні системи.

Угода про заснування Центру кіберзахисту (2014) – Угода, укладена між ЄС і деякими державами-членами, згідно з якою був заснований Центр кіберзахисту як платформа для обміну інформацією та співпраці в сфері кібербезпеки.

Директива ЄС про мережеву та інформаційну безпеку (NIS Directive, 2016) – Директива ЄС, що створює механізми для забезпечення високого рівня кібербезпеки в критичних секторах, таких як енергетика, транспорт, фінанси. Вона також визначає обов'язки для держав-членів ЄС. Країни ЄС, впроваджуючи цю директиву, покращили рівень кібербезпеки в критичних секторах, зменшивши ризики та збільшивши відповідальність підприємств.

2. Міжнародні організації

Міжнародні організації відіграють важливу роль у координації міжнародних зусиль з підвищення рівня кібербезпеки, розробці політик, стандартів, а також у сприянні міждержавному співробітництву в цій сфері. Нижче наведено приклади конкретних дій та ініціатив деяких ключових міжнародних організацій у галузі інформаційної безпеки.

Організація Об'єднаних Націй (ООН) активно працює над питаннями глобальної кібербезпеки через різні структурні підрозділи, такі як Офіс Верховного представника ООН з питань роззброєння (UNODA). У 2015 році Група урядових експертів (GGE), створена під егідою ООН, оприлюднила звіт з рекомендаціями щодо відповідальної поведінки держав у кіберпросторі, що заклала основу для міжнародного діалогу з кібербезпеки.

Міжнародний союз електрозв'язку (англ. International Telecommunication Union, ITU) – це спеціалізоване агентство ООН, що відповідає за питання, пов'язані з інформаційними та комунікаційними технологіями, включаючи стандартизацію та розвиток кібербезпеки. ITU розробляє глобальні стандарти захисту даних та кібербезпеки, такі як X.509 для цифрових сертифікатів і шифрування, що є фундаментом для безпечного обміну даними в Інтернеті.

Північноатлантичний альянс (НАТО) посилює колективну кібероборону через обмін розвідданими, спільні навчання та захист критичної інфраструктури альянсу. НАТО створило Центр відмінності з кібероборони (CCDCOE) в Таллінні, Естонія, що слугує майданчиком для навчання, досліджень та розробки у сфері кібероборони (Давиденко, 2021).

Організація з безпеки та співробітництва в Європі (ОБСЄ) також має значний вплив на розвиток міжнародної інформаційної безпеки, хоча її пряме призначення не обмежується лише кібербезпекою. Одним із прикладів діяльності ОБСЄ в цій сфері є розробка і ухвалення «Конфіденційних заходів збільшення довіри у сфері кібер/ІКТ-безпеки», які включають заходи для обміну інформацією про національні кібербезпекові політики, обмін досвідом щодо кіберінцидентів та спільне використання кращих практик у сфері кіберзахисту. Ці заходи спрямовані на зменшення непорозумінь та підвищення рівня довіри між державами, що є ключовим фактором для запобігання конфліктів у кіберпросторі.

3. Національні законодавства

Національні законодавства у сфері інформаційної безпеки відрізняються від країни до країни, але всі вони покликані забезпечити захист інформації та інформаційних систем на території держави (Коваленко, 2022). Ці закони зазвичай охоплюють широкий спектр питань: від захисту даних персонального характеру до кіберзлочинності та кібероборони. Закон про захист інформаційної інфраструктури критичної важливості (CISA, 2018 р.) – Закон спрямований на покращення безпеки національних критично важливих інфраструктур шляхом співпраці між урядом і приватним сектором; Загальний регламент про захист даних (GDPR, 2018 р.) – одна з найбільш впливових нормативних угод у світі щодо захисту даних, що встановлює високі вимоги до обробки персональних даних організаціями всередині та поза ЄС; Директива NIS (2016 р.) – спрямована на підвищення рівня національної кібербезпеки та сприяє обміну інформацією про кіберзагрози між країнами ЄС (Давиденко, 2021).

4. Стандарти та протоколи інформаційної безпеки

Стандарти та протоколи у сфері інформаційної безпеки є основою для забезпечення надійного захисту інформаційних систем і даних у глобальному масштабі. Вони визначають вимоги до менеджменту безпеки, криптографічного захисту даних, а також процедури і технології, які допомагають запобігти кібератакам та забезпечують конфіденційність, цілісність і доступність інформації. Розглянемо детально декілька з них.

ISO/IEC 27001 – це міжнародний стандарт, який встановлює вимоги до системи управління інформаційною безпекою (ISMS). Він допомагає організаціям встановити, реалізувати, підтримувати та постійно вдосконалювати ISMS. Реалізація ISO/IEC 27001 дозволяє організаціям керувати ризиками безпеки своїх інформаційних активів. Прикладом може слугувати компанія Microsoft, яка використовує цей стандарт для захисту інформації у своїх хмарних сервісах, таких як Azure та Office 365.

SSL/TLS – це криптографічні протоколи, які забезпечують захищене з'єднання між вебсервером і браузером. Вони широко використовуються для забезпечення захисту Інтернет-транзакцій, наприклад, під час онлайн-покупок або банківських операцій. Використання SSL/TLS гарантує, що всі передані дані зашифровані і не можуть бути прочитані або змінені зловмисниками. Amazon використовує SSL/TLS для безпеки покупок на своєму вебсайті.

HTTPS – розширення протоколу HTTP з використанням SSL/TLS для шифрування даних. HTTPS захищає конфіденційність даних користувачів під час роботи в мережі Інтернет. Google робить HTTPS обов'язковим для всіх сайтів, які індексуються його пошуковою системою, щоб гарантувати безпечніший вебдосвід для користувачів.

5. Технологічні рішення

Таблиця 2.1

Технологічні рішення для забезпечення інформаційної безпеки

Технологічне рішення	Приклад компанії	Застосування

Шифрування	WhatsApp	Конфіденційність повідомлень та даних
Блокчейн	IBM Food Trust	Відстеження ланцюга постачання продуктів
Штучний інтелект	Darktrace	Виявлення та захист від кіберзагроз

Шифрування використовується для захисту конфіденційності, блокчейн – для забезпечення цілісності та невідмінності даних, а штучний інтелект допомагає виявляти та відвертати кіберзагрози. Ці інноваційні підходи сприяють вдосконаленню інформаційної безпеки на рівні глобальних стандартів.

6. Співробітництво між секторами

Ефективна взаємодія між державним сектором, приватним сектором та громадянським суспільством є ключем до успішної реалізації цілей інформаційної безпеки. Розвиток міжнародної архітектури кібербезпеки визначається взаємодією міжнародних організацій, угодами та ініціативами країн для забезпечення ефективності заходів у сфері кібербезпеки. Спільні стандарти, обмін інформацією та співпраця між державами стають ключовими складовими глобального відповідного відгуку на кіберзагрози

2.3. Вплив кіберзагроз на міжнародні відносини та національну безпеку

У сучасному світі існує безліч способів маніпулювання інформацією. Технології маніпуляції все частіше використовуються для інформаційних війн, ліквідації конкурентів, впливу на маси та реалізації інших завдань. Останнім часом інформаційний тероризм набуває ще більшої популярності (Давиденко, 2021).

Інформаційний тероризм виходить за межі кіберзлочинності, хоча вона є його невід'ємною частиною. Він також охоплює маніпуляції з інформацією або її фальсифікацію та, у деяких випадках, розповсюдження завідомо неправдивих даних. Вплив інформаційних порушень на безпеку країни є значним не тільки через

економічні збитки, а й через порушення функціонування інформаційно-комунікаційних систем і поширення незаконного контенту (Антонюк, 2021).

В історії політичної боротьби тероризм відзначається особливістю тим, що досягнення політичних цілей настає через непрямий вплив. Суттєва різниця тероризму від інших форм жорстокої політичної конфронтації полягає в його відмові від прямого використання насильства проти цивільного населення, замість чого він використовує інші стратегії для досягнення своїх політичних цілей.

Міжнародні експерти у сфері боротьби з інформаційними загрозами визначають інформаційний тероризм як синтез фізичного насильства та недобросовісного використання інформаційних систем. Також це охоплює умисне зловживання цифровими інформаційними системами, мережами чи їхніми компонентами з метою сприяння терористичним операціям чи діям (Коваленко, 2022).

Сучасний інформаційний тероризм визначається як комплекс інформаційних воєн і спеціальних операцій, що пов'язані з діяльністю національних або транснаціональних злочинних структур та апаратів спецслужб іноземних держав. На сучасному етапі широко використовується інформаційний тероризм, а також новітні засоби зв’язку для полегшення процесу планування операцій, проведення зборів, комунікації, передачі оперативної інформації тощо. Вплив медіа-тероризму призводить до того, що особа губиться в необмеженому інформаційному просторі, де ЗМІ функціонують як інструменти конструювання необ’єктивної реальності. Головною метою цієї зконструйованої реальності є приховування істини шляхом використання «м'якої сили», спрямованої на підкорення особи за допомогою упереджених суджень. Унаслідок цього важко говорити про перехід значної кількості інформації в якість, особливо в контексті ЗМІ, зокрема Інтернету, що служить платформою для політичних ігор, спрямованих на спотворення реального стану речей (Давиденко, 2021).

Проте визначення терміну «кібертероризм» викликає певні труднощі, оскільки важко відмежувати його від інших явищ, таких як інформаційна війна чи кіберзлочинність. Кіберзлочинність охоплює незаконні дії, вчинені особами, які

використовують інформаційні технології у злочинних цілях. Серед основних видів кіберзлочинності можна виокремити поширення шкідливого програмного забезпечення, злам паролів, крадіжку банківської інформації (номерів кредитних карток та інші) та незаконне розповсюдження інформації через Інтернет. У цьому контексті важливо розрізняти ці поняття для більш точного розуміння природи та масштабів кібертероризму в сучасному світі (Таблиця 2.2).

Таблиця 2.2

Види кібертероризму

Вид кібертероризму	Опис	Характеристики
Простий	цей тип кібертероризму є неструктурованим і зазвичай включає в себе використання хаків проти інформаційних систем, при цьому використовуються програми, створені іншими особами.	Це найпростіший вид атаки з мінімальними або незначними втратами.
Розширений	Структурований тип, який дозволяє здійснювати складні атаки проти кількох систем або мереж. Можливе змінення або створення основних інструментів злому.	Цей вид має структуру та управління, члени таких груп можуть навчати нових хакерів.
Комплексний	Координований вид, який може спричинити серйозні порушення в системі безпеки країни. Має можливість створення складних інструментів злому.	Має жорстку структуру і часто являє собою організацію, яка вміє тверезо аналізувати свої дії та розробляти плани атак.

Тривожна статистика кібератак в українському інфопросторі відображає великий масштаб проблеми: протягом першої половини 2022 року було зафіксовано

236,1 мільйона атак програм-вимагачів по всьому світу, що створює надзвичайно загрозливу обстановку. Наслідки цих атак виявляються у фінансових втратах, порушенні конфіденційності та крадіжках особистих даних. Малі та середні підприємства, які часто є джерелом економічного життя, стають особливо привабливими цілями через цінні активи даних та обмежені ресурси в галузі кібербезпеки (Кібербезпека в інформаційному суспільстві, 2023).

Дослідження виявили, що непропорційно велика частка кібератак, а саме 43%, спрямована на малий бізнес, що може призвести до негативних наслідків для таких компаній, включаючи фінансові збитки та репутаційні втрати. З іншого боку, великі корпорації стикаються з кіберзагрозами на масштабному рівні та інвестують величезні ресурси в кібербезпеку для захисту своєї інформації та систем. Незважаючи на це, у 2020 році середні втрати від витоку даних для таких компаній склали приблизно 3,86 мільйона доларів за кожен інцидент, підкреслюючи необхідність захищати не тільки фінансові активи, але й репутацію бренду та довіру клієнтів на довготривалу перспективу (Давиденко, 2021).

Кібератака «NotPetya», що спостерігалася в Україні у 2017 році, визначається як одна з найбільш руйнівних та впливових в історії кіберзлочинності. Ця атака, використовуючи вразливості в програмному забезпеченні, миттєво поширилася, атакуючи тисячі комп'ютерів. Що стосується методів, «NotPetya» використовувала техніку есперадо, швидко розповсюджуючись під прикриттям легітимних програмних оновлень. Наслідки атаки були руйнівними, спричинивши паралізацію систем урядових установ і фінансових компаній в Україні. Однак важливо відзначити, що вплив атаки виявився глобальним, оскільки вона зачепила комп'ютери по всьому світу (Антонюк, 2021).

2.4. Кібершпигунство та вплив на геополітику

У сучасному світі кібершпигунство вийшло далеко за межі звичайного збору інформації, ставши миттєвим інструментом впливу на різноманітні сфери. Воно впливає на геополітичну картину через декілька ключових аспектів. По-перше, кібершпигунство використовується для здобуття стратегічно важливої інформації, такої як військові плани, політичні стратегії та економічні наміри. Це відкриває можливості для держав отримувати перевагу в міжнародних відносинах і визначати свою політику (Житник, 2021). Окрім цього, кібершпигунство стає інструментом впливу на політичні процеси та виборчі кампанії. Зловмисники можуть використовувати кіберзасоби для маніпулювання громадською думкою, підриву демократичних інститутів і навіть зміни політичної орієнтації країн (Коваленко, 2022).

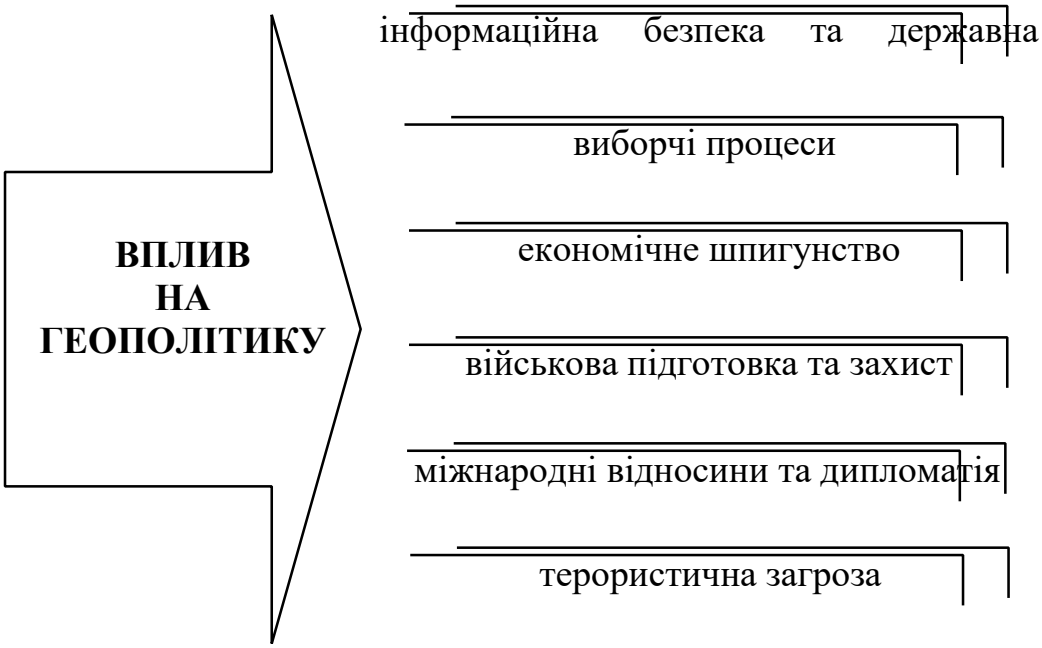

Рис.2.2 Вплив на геополітику

Кібершпигунство, як частина кібероперацій, є ефективним інструментом для країн, які прагнуть отримувати *конкурентну перевагу та вплив у світових справах*. Це визначається здатністю здійснювати таємні інформаційні вторгнення в інші

держави, таємно здобуваючи конфіденційні дані та таємниці (Житник, 2021). Проаналізуємо кілька прикладів кібершпигунства, що суттєво вплинули на світову політику та безпеку:

У 2015 році кібератака на Офіс Управління Персоналом в США була організована для отримання даних, пов'язаних із секретами безпеки та персональними даними службовців. Це призвело до збитків у вигляді втрати довіри та витоку конфіденційної інформації. Між 2015 і 2018 роками в Німеччині розкрили випадки кібершпигунства, які були приписані кібергрупі APT28, пов'язаній з російськими спецслужбами. Атака була спрямована на отримання конфіденційної інформації та вплив на політичні рішення.

Створений, імовірно, США та Ізраїлем, Stuxnet (2010) визначив новий рівень кібершпигунства. Цей вірус призначався для впливу на іранську ядерну програму, вражаючи комп'ютери, що керують центрифугами. Це стало прикладом військового використання кіберзброї. У 2018 році виявлено кібератаки на Офіс ЄС, що мали на меті отримання конфіденційної інформації. Хоча атаки не були пов'язані з конкретною країною, вони викликали питання щодо кібербезпеки в європейському просторі (Кібербезпека в інформаційному суспільстві, 2023).

Кібершпигунство стає ефективним інструментом для втручання в *політичні процеси та формування громадської думки*. Розглянемо конкретні приклади, де цей вид кібероперацій використовувався для досягнення політичної мети. Один із найвідоміших прикладів – це втручання росії у виборчий процес у Сполучених Штатах у 2016 році. Російське кіберугруповання Fancy Bear, пов'язане з російськими спецслужбами, здійснювала кібершпигунство, викрадаючи електронні листи та інші конфіденційні дані та публікуючи їх для впливу на виборчий процес та формування громадської думки. Перед президентськими виборами у Франції 2017 року виникли кібератаки на політичні партії та виборчий штаб Еммануеля Макрона. Результатом цих атак був витік конфіденційної інформації, спрямований на підрив репутації кандидата. Росія використовує кібершпигунство і у війні в Україні: зламані електронні системи та розповсюдження дезінформації спрямовані на вплив на політичний ландшафт та формування громадської думки. Перед російсько-

грузинською війною 2008 року, росія здійснила кібератаки на грузинські військові та господарські об'єкти, що були спрямовані на паралізування інфраструктури та втручання у військові операції (Антонюк, 2021).

Таблиця 2.3

Приклади кібершпигунства

Приклади	Рік	Опис та наслідки атак
Атака на SolarWinds	2020	Спроба шпигунства проти урядових агенцій США та приватних компаній. Зловмисники отримали доступ до конфіденційної інформації, включаючи інновації та стратегічні плани. (Коваленко, 2022).
Хакерська атака на Nortel Networks	2018	Канадський телекомунікаційний гігант Nortel став жертвою тривалого шпигунства. Зловмисники отримали доступ до документів компанії, що включало дослідження та розробки, призводячи до банкрутства. (Житник, 2021).
Атаки на Equifax	2017	Витік даних у компанії Equifax призвів до розголошення конфіденційної інформації 147 мільйонів американців, підірвавши фінансову стабільність та репутацію корпорації. (Житник, 2021).
Витік інформації з Sony Pictures	2014	Атака на Sony Pictures призвела до витоку конфіденційної інформації, включаючи персональні дані співробітників та електронні листи керівництва, що вплинуло на репутацію та фінансовий стан компанії. (Коваленко, 2022).

Кібершпигунство, націлене на владні структури та конфіденційні дані країн, *може суттєво вплинути на міжнародні відносини*, порушуючи довіру та

викликаючи необхідність дипломатичних заходів. Реальні приклади, які ілюструють цей аспект кібершпигунства наведені в Таблиці 2.4.

Таблиця 2.4

Кібершпигунство, націлене на владні структури і конфіденційні дані країн

Приклади	Рік	Опис та наслідки атак
Кібершпигунство на виборчі процеси в Сполученому Королівстві	2019	У 2019 році було виявлено спроби кібершпигунства в Сполученому Королівстві, спрямовані на виборчі процеси. Хакерські групи намагалися отримати доступ до конфіденційної інформації, пов'язаної з політичними стратегіями. Це призвело до збільшення обережності та заходів кібербезпеки в уряді та суспільстві (Антонюк, 2021).
російська кібершпигунська атака на Офіс президента Франції	2017	У 2017 році під час президентських виборів у Франції сталася серйозна кібершпигунська атака, метою якої було отримання конфіденційної інформації, пов'язаної з виборчим процесом і політичними стратегіями. Ця атака викликала напругу в міжнародних відносинах, а Париж офіційно звинуватив росію в спробах втручання у внутрішні справи Франції. (Коваленко, 2022).
Румунський інцидент з кібершпигунством	2016	Румунія звинуватила Росію в кібершпигунстві, у результаті чого було викрадено конфіденційні дані та документи з урядових інституцій. Цей інцидент порушив відносини між країнами та призвів до дипломатичної напруги (Антонюк, 2021).
Кібершпигунство проти урядів	2013	Група хакерів, яку пов'язують з Північною Кореєю, виконала серію кібершпигунських атак

Південної Кореї та США		на уряди Південної Кореї та США. Однією з основних цілей було отримання конфіденційної інформації. Ці атаки створили напругу в регіональних відносинах і призвели до висловлення обвинувачень і санкцій. (Коваленко, 2022).

Сучасні фахівці зафіксували збільшення кількості кіберінцидентів та кібератак, спрямованих проти державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури в Україні. Про це повідомлено Державною службою спеціального зв’язку та захисту інформації. За допомогою системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було оброблено 24 мільярди подій інформаційної безпеки. Кількість зареєстрованих та оброблених кіберінцидентів зросла з 64 до 115 порівняно з попереднім кварталом. Головною метою хакерів залишається кібершпіонаж, порушення доступності державних інформаційних сервісів і знищення даних інформаційних систем.

Експерти з Державного центру кіберзахисту спостерігають значне збільшення поширення шкідливого програмного забезпечення, що дозволяє зловмисникам викрадати або навіть видаляти дані. Важливо відзначити, що протягом цих місяців кількість критичних подій у сфері інформаційної безпеки, за якими стоять IP-адреси з росії, збільшилася у 35 разів у порівнянні з першими двома кварталами 2022 року (Кібербезпека в інформаційному суспільстві, 2023).

Кібершпигунство має глибокий вплив на геополітичний ландшафт, посилюючи напруженість між державами та впливаючи на міжнародні відносини. Через здатність анонімно проникати в інформаційні системи, держави використовують кібершпигунство для збору розвідданих, впливу на політичні процеси, економічну стабільність та національну безпеку інших країн. Це веде до ескалації конфліктів, зростання міжнародної напруженості та потреби в посиленні кіберзахисту.

Висновок до другого розділу

1. Міжнародні організації, які не адаптуються до сучасних викликів, стають менш авторитетними, у той час як ті, що гнучко адаптують свою діяльність до новітніх вимог, збільшують свій вплив. ООН, ЄС, ОБСЄ та інші міжнародні інституції відіграють важливу роль у формуванні базових принципів та норм, спрямованих на зміцнення кібербезпеки. Хоча вони і виступають ініціаторами ухвалення міжнародних конвенцій, створення регулятивних рамок і рекомендацій, що сприяють підвищенню рівня захисту кіберпростору, ці організації досі не запровадили ефективний міжнародно-правовий механізм, спрямований на оптимізацію проблем кібербезпеки.

2. Вплив кіберзагроз на міжнародні відносини та національну безпеку сьогодні є не тільки значущим, але й невпинно зростає. Кібератаки стають не лише інструментом дестабілізації міжнародного порядку, але й серйозною загрозою для внутрішньої стійкості держав. Розвиток і вдосконалення міжнародних стратегій, співпраця між країнами, а також внутрішні заходи для зміцнення кібербезпеки стають невід'ємною частиною зусиль, спрямованих на забезпечення стійкості та захисту національних інтересів в умовах високотехнологічних загроз.

3. Розбір концепції інформаційного тероризму критично важливий для глибшого розуміння сутності сучасного міжнародного тероризму, виявлення та нейтралізації загроз, що можуть підірвати стабільність держав і засади національної безпеки. Кібершпигунство суттєво переплітається з геополітикою, створюючи нові виклики й загрози для держав. Ця форма кібератак впливає на безпеку, конкурентоспроможність та довіру міжнародних гравців, порушуючи звичні дипломатичні норми. Гарантування кібербезпеки стає стратегічним завданням для держав, які прагнуть утримати стабільність і вплив у сучасному світі, де віртуальна арена дипломатії та міжнародних конфліктів набуває все більшого значення.

4. Кібершпигунство наразі – це не лише про збір інформації, а й про маніпулювання громадською думкою, підриву демократичних інститутів і навіть зміни політичної орієнтації країн. Результатами застосування кібершпигунства

може бути не просто витік інформації, а й підрив репутації кандидата на виборах, паралізування різного виду інфраструктури, втручання у військові операції та втрата довіри громадян до уряду або навіть між державами.

РОЗДІЛ 3

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА КІБЕРБЕЗПЕКА В УКРАЇНІ

3.1. Аналіз участі України в міжнародних ініціативах з кібербезпеки

У сучасному світі, де кіберзагрози набувають усе більшої складності та масштабів, участь у міжнародних ініціативах з кібербезпеки стає критично важливою для кожної держави. Розбіжності в міжнародному законодавстві та відсутність уніфікованих нормативів спонукають уряди країн розробляти власну політику у сфері кібербезпеки на національному рівні. Більшість країн світу вже створили спеціалізовані відомства, включаючи як правоохоронні, так і військові органи для захисту від кіберзагроз і розробки оборонних технологій.

Україна, яка перебуває у фокусі численних кібератак, що не тільки становлять загрозу національній безпеці, але і впливають на міжнародні відносини, активно долучається до глобальних зусиль зі створення безпечного кіберпростору.

Стаття 14 Закону України «Про основні засади забезпечення кібербезпеки України» встановлює, що Україна реалізує міжнародне співробітництво в галузі кібербезпеки на основі міжнародних договорів, укладених з іншими країнами, їхніми правоохоронними відомствами та спецслужбами, а також з міжнародними організаціями, що борються з транснаціональною кіберзлочинністю.

Відповідаючи на потребу підвищення рівня кібербезпеки, особливо через міжнародне співробітництво, Президент України Володимир Зеленський 20 грудня 2019 року підписав указ, завдяки якому набуло чинності рішення Ради Національної безпеки і оборони від 7 грудня 2019 року щодо невідкладних заходів з посилення державних можливостей у сфері кібербезпеки. Відповідно до основних доктрин і чинного законодавства, Україна співпрацює в цій галузі з іноземними країнами, зокрема з членами НАТО та ЄС, їхніми військовими формуваннями,

правоохоронними та спеціальними службами, а також з міжнародними організаціями на основі укладених міжнародних договорів.

Інформація щодо гарантування кібербезпеки, боротьби з міжнародною кіберзлочинністю та кібертероризмом передається іноземним партнерам на підставі укладених Україною міжнародних договорів. Цей підхід включає широкий спектр нормативних, методичних, практичних, наукових та освітніх напрямів, що передбачає проведення міжнародних семінарів і конференцій, надання методичної та практичної підтримки іноземним партнерам, організацію робочих зв'язків з провідними експертами в галузі кібербезпеки (Vevera, 2018).

У контексті глобальних кіберзагроз і постійної еволюції кіберпростору Україна активно розвиває співпрацю з міжнародними партнерами, включаючи країни Європейського Союзу, Сполучені Штати Америки, а також з міжнародними організаціями, такими як ООН, ОБСЄ, та Європейське агентство з мережевої та інформаційної безпеки (ENISA).

Одним із прикладів міжнародної співпраці є участь України в програмах підвищення кібербезпеки, спонсорованих ЄС та НАТО, зокрема в ініціативах, спрямованих на підвищення захисту критично важливої інфраструктури. Це включає розробку спільних навчальних програм, обмін кращими практиками у сфері кіберзахисту та надання технічної допомоги. Україні рекомендовано не лише продовжувати процес трансформування свого законодавства у відповідності до директив ЄС, але й інтегрувати сучасні досягнення міжнародних організацій, розвиток міжнародного права в цій сфері та досвід міжнародних судових органів (Кібербезпека в інформаційному суспільстві, 2023).

Враховуючи сучасні виклики та загрози, для України важливо брати участь у роботі міжнародної платформи, такої як Програма дій зі стимулювання відповідальної поведінки держав у кіберпросторі, що ведеться Генеральною Асамблеєю ООН та Групою урядових експертів ООН з питань інформаційної безпеки (UNGGE).

Для України одним із основних напрямів міжнародної співпраці у сфері кібербезпеки, зокрема, залишається стратегічне партнерство з Північноатлантичним

Альянсом. У рамках цього співробітництва виокремлюються наступні ключові завдання між НАТО та його партнерами в галузі кіберзахисту:

- підтримка стабільної роботи об’єктів критичної інформаційно-комунікаційної інфраструктури;
- розроблення ефективних стратегій протидії кібератакам;
- допомога державам-членам у відновленні стабільної роботи інфраструктури після зовнішніх кібернетичних атак;
- забезпечення швидкого реагування на кіберзагрози для інформаційної безпеки держав-членів.

У контексті стратегічного розвитку співпраці між Україною та НАТО, важливо врахувати актуальні тенденції в цій галузі. Основні вектори подальшої взаємодії можуть включати:

- адаптацію передового досвіду НАТО та розвиток державно-приватного партнерства;
- залучення України до Центру передового досвіду НАТО з кібероборони для імплементації кращих практик та зміцнення співпраці у сфері кібербезпеки;
- підвищення оборонного та технічного потенціалу України у кібербезпеці за підтримки Трастового фонду НАТО та співпраці з Румунією;
- розробка механізмів розподілу ризиків за допомогою захищених хмарних сервісів для зниження потенційних збитків від кібератак на інформаційні системи держави;
- впровадження кращих практик для посилення міжвідомчої кооперації і створення ефективних механізмів їх використання;
- спільне вироблення мотиваційної системи для професіоналів у галузі кібербезпеки (Коваленко, 2022).

На сучасному етапі перед українським політичним керівництвом стоїть відповідальне завдання інтегрувати передовий міжнародний досвід і, спільно з глобальним співтовариством, активізувати заходи проти глобальної кіберзлочинності. Це включає:

- створення та інтеграцію ефективної моделі національної системи кібербезпеки в рамках співпраці з НАТО;
- взаємодію та співпрацю з європейськими організаціями, що займаються питаннями кібербезпеки;
- розробку і впровадження міжнародно-правових механізмів для забезпечення кібербезпеки на території України;
- використання міжнародної технічної допомоги та грантів для розвитку національної кібербезпеки в рамках комплексних міжурядових програм;
- посилення співпраці з НАТО для зміцнення стійкості та підвищення спроможностей України у сфері кібербезпеки.

На початку 2020 року Україна розпочала співпрацю з Японією, спрямовану на зміцнення здатності обох держав протистояти кіберзагрозам та розробку спільних ініціатив у цій галузі. Очікується, що це двостороннє співробітництво допоможе обом державам краще планувати й реагувати на майбутні кіберзагрози. У результаті, Україна та Японія домовилися про тісну взаємодію між компетентними органами, щоб створити відкритий, операційно сумісний, надійний і безпечний кіберпростір.

Діалог з приватним сектором, академічними кругами та неурядовими організаціями також відіграє важливу роль у зміцненні кібербезпеки в Україні. Проекти, такі як створення спільних дослідницьких центрів, запуск освітніх програм і курсів з кібербезпеки в університетах та розвиток стартапів у галузі кібербезпеки, підкреслюють цю співпрацю. Великі IT-компанії, такі як Microsoft та Google, проводили в Україні навчальні сесії та семінари, спрямовані на підвищення рівня кібергігієни серед користувачів та організацій.

3.2. Кіберзагрози та виклики для України

Україна, як держава з розвиненою IT-індустрією та стратегічним геополітичним розташуванням, стикається з численними кіберзагрозами, що

вимагають ефективного реагування та адаптації. У цьому контексті МЦБ стає не тільки технологічним викликом, а й політичним, економічним і соціальним питанням, що вимагає комплексного підходу та постійної уваги на всіх рівнях управління.

Російська активність у кіберпросторі є основним викликом і загрозою для кібербезпеки України. Починаючи з 2014 року, у контексті гібридної війни проти України, росія активно використовує кібернапади на сайти урядових установ та інфраструктуру, створюючи серйозні загрози для національної безпеки. Подібні атаки не нові: у 2008 році, під час війни проти Грузії, російські хакери вчинили подібні атаки на відомчі сайти та ЗМІ, спричинивши перебої в роботі, а також провели DoS-атаки на приватні структури (Кібербезпека в інформаційному суспільстві, 2023).

Кіберпростір використовується рф для здійснення розвідувально-підривної діяльності проти України, а також для проведення спеціальних операцій з прихованого проникнення в кібермережі органів державного управління. Ці дії включають установлення дистанційного контролю над об’єктами критичної інфраструктури з метою досягнення стратегічних переваг та захисту інтересів у різних сферах, таких як інформаційна, військово-політична, фінансово-економічна та енергетична. Відомо, що рф розробила кіберзброю для нейтралізації об’єктів критичної інфраструктури суперника з метою збільшення ефективності першого удару або максимального ослаблення його обороноздатності.

Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA веде моніторинг діяльності понад 80 хакерських груп, більшість з яких є угрупованнями з рф, а 90% їхніх учасників складають російські військові.

З початком повномасштабної війни росії проти України сталися наступні інциденти, пов’язані з кібербезпекою: злам систем зв’язку газети «Kyiv Post» та супутникової мережі «KA-SAT» за годину до початку вторгнення 24 лютого, кібератака IssacWiper на державні вебсайти 25 лютого, кібернапад на прикордонний пункт з метою ускладнення виїзду біженців до Румунії того ж дня, а також атаки на цифрову інфраструктуру України 28 лютого, що призвели до перебоїв у доступі до

фінансових та енергетичних послуг (Кібербезпека в інформаційному суспільстві, 2023).

Окрім цього, були здійснені фішингові атаки на громадян та державні служби, а також на постачальників телекомунікаційних послуг, що призвело до перебоїв у функціонуванні українських мереж. Наприкінці березня шкідливе програмне забезпечення CaddyWiper вразило системи кількох українських установ державного та фінансового сектору. Через два дні на одному з українських телеканалів з'явилось фальшиве повідомлення, нібито Президент України Володимир Зеленський закликав народ до капітуляції. Окрім того, дипфейкове відео із Зеленським поширили через один із Telegram-каналів (Кібербезпека в інформаційному суспільстві, 2023).

З кінця березня кібератаки на Україну охопили фішингові атаки на електронні адреси уряду та збройних сил (17 березня 2022) та на інші організації (18 березня 2022), а також застосування бекдора LoadEdge дозволило зловмисникам встановити шпигунське програмне забезпечення (20 березня 2022). Напади на сайти Укртелекому та WordPress викликали збої у зв'язку та обмежили доступ до фінансових і урядових вебресурсів (28 березня 2022). За допомогою інформаційного викрадача MarsStealer 30 березня 2022 було отримано доступ до особистих даних українських громадян та організацій. У квітні хакери також захопили банківські та платіжні дані через троянські програми (14 квітня 2022) і фальшиві опитування в соціальних мережах (19 квітня 2022) (Пшетачник, 2022).

Деякі кібератаки були націлені на завдання шкоди цивільному населенню. Наприклад, 8 квітня 2022 була здійснена спроба заблокувати роботу електростанцій, що могло призвести до відключення електропостачання для мільйонів людей. 22 квітня 2022 внаслідок кібернападу було тимчасово припинено роботу української поштової служби, що сталася під час випуску поштових марок, присвячених війні. У травні, під час військових дій, були здійснені атаки на урядові вебсайти, телекомунікаційні послуги та інфраструктуру. Зокрема, атака на Одеську міську раду збіглася з ракетними ударами по житлових районах міста 7 травня. 9 травня хакери організували розподілену DDoS-атаку на декілька українських

телекомунікаційних операторів, метою якої було перенаправлення та фільтрація Інтернет-трафіку до окупованих територій (Коваленко, 2022).

Неможливо пройти повз найбільшої, за словами президента компанії “Київстар” Олександра Комарова, у світі хакерської атаки на телеком-інфраструктуру – атаки на найбільшого в Україні оператора зв’язку 12 грудня 2023 року. Напад на віртуальну інфраструктуру “Київстару” завершився не лише зникненням мобільного зв’язку та Інтернету, а й підривом роботи банківської системи, виведення з ладу охоронних систем і гарячих ліній в уряді України. Зокрема, у деяких містах довелося застосовувати механічне відключення вуличного освітлення. Відповідальність за скоєний злочин на себе взяло російське кіберзлочинне угруповання “Солнцепек” (Forbes Україна, 2023). Хакерська атака на ІТ-інфраструктуру оператора зв’язку вкотре доводить, що з дедалі більшою інформатизацією та автоматизацією людство набуває знань і можливостей з одного боку, та з іншого, – стикається із загрозами та щоразу вищою вразливістю. Інформаційна зброя наразі здатна паралізувати державу зсередини, руйнуючи її критичну, виробничу, соціальну інфраструктури та безпосередньо впливаючи на ситуацію на фізичному фронті.

Також викликає тривогу присутність на українському ринку мобільних комунікаційних засобів, вироблених у Китаї, зі вбудованим програмним забезпеченням. У контексті глобальних досліджень в Європі та США, які виявили потенційні ризики таких продуктів для збору даних, для України стає критично важливим зміцнювати співпрацю з НАТО, щоб уникнути негативних наслідків від їх масового розповсюдження і виключити можливість використання таких засобів і програм у державному та військовому секторах. Зокрема, у січні 2021 року Генеральний секретар НАТО Єнс Столтенберг закликав країни-члени Військового комітету альянсу збільшувати оборонні витрати та інвестувати в новітні технології на тлі російської агресії та зростанні впливу Китаю (Пшетачник, 2022).

3.3. Основні принципи та завдання Стратегії кібербезпеки України

Національна інформаційна безпека – це багатогранне поняття, яке по-різному трактується в публічних документах, академічних виданнях та експертних аналізах. Це поняття виходить за рамки забезпечення лише інформаційної безпеки держави, її установ, оборонного та внутрішньополітичного секторів. Доктрина національної інформаційної безпеки враховує захист інтересів індивідів, суспільства й держави та включає захист інформаційної інфраструктури за допомогою програмних, фізичних і технічних засобів.

Указом Президента України Петра Порошенка від 27 січня 2016 року «Про рішення РНБОУ від 27 січня 2016 року» запроваджено Стратегію кібербезпеки України. Стратегія, розроблена фахівцями в галузі кібербезпеки та затверджена на засіданні РНБОУ, спирається на положення Конвенції про кіберзлочинність, яку Україна ратифікувала Законом № 2824-IV від 7 вересня 2005 року. Офіційно Стратегія набула чинності 15 березня 2016 року та включає комплексний набір заходів і пріоритетів для забезпечення захисту кіберпростору, які охоплюють:

- розробку та швидку адаптацію національної політики для розвитку кіберпростору та забезпечення відповідності стандартам ЄС та НАТО;
- створення національної нормативно-правової бази та уніфікацію термінології у сфері кібербезпеки;
- формування конкурентоспроможного ринку електронних комунікацій;
- розвиток технологій захисту в мобільному зв'язку, включаючи апаратну безпеку, безпеку контенту, додатків та комунікаційних сервісів;
- підвищення рівня цифрової грамотності населення та культури безпечної поведінки в кіберпросторі;
- проведення тренінгів з реагування на надзвичайні ситуації та інциденти в кіберпросторі;
- зміцнення міжнародного співробітництва, підтримка глобальних ініціатив у сфері кібербезпеки та посилення взаємодії України з ЄС та НАТО (Піпченко, Рижков, 2021).

Стратегія передбачає створення системи «активного кіберзахисту», яка включатиме воєнно-політичні, військово-технічні та інші заходи. Це має на меті розширити можливості військових і безпекових структур у кіберпросторі, а також створення й розвиток сил і засобів для можливого реагування на агресію у віртуальному світі, як засобу стримування воєнних загроз. З іншого боку, розвиток такого механізму вимагає значних інвестицій і глибоких знань (Коваленко, 2022).

Одним із перших етапів у впровадженні Стратегії було утворення в червні 2016 року Національного координаційного центру кібербезпеки, який діє як робочий орган Ради національної безпеки і оборони України. У цілому, структура Стратегії більше нагадує концепцію або декларацію, ніж законодавчий акт. Для її втілення необхідно внести низку змін до українського законодавства, які не лише створять основу для реалізації положень Стратегії, а й посилять відповідальність за порушення в сфері кібербезпеки.

Однак документ мав декілька недоліків: по-перше, стратегія не мала чітко визначених державних пріоритетів у кіберсекторі. По-друге, зосередження уваги на діяльності органів безпеки та оборони відбувалося без належної розробки моделі державно-приватного партнерства та обмежене залучення академічних кіл та громадськості. По-третє, стратегія не включала систему індикаторів, яка б дозволяла оцінювати виконання завдань та стан кібербезпеки загалом.

Однак слід відмітити, що протягом цього періоду сталося кілька значущих змін у розвитку кібербезпеки України:

- у 2017 році було ухвалено Закон України «Про основні засади забезпечення кібербезпеки України», який встановив повноваження державних органів, підприємств та осіб у цій сфері;
- у 2020 році Кабінет Міністрів України рішенням №943 затвердив механізм формування переліку об’єктів критичної інформаційної інфраструктури, хоча сам перелік так і не був створений;
- у низці державних установ, включно з Національним банком, Міністерством інфраструктури, Державною службою спецзв’язку та СБУ, були створені спеціалізовані підрозділи, а також робочий орган РНБО – Національний

координаційний центр кібербезпеки, що займається координацією дій різних учасників у цій сфері;

- розроблено міжнародне партнерство в галузі кібербезпеки, зокрема було розпочато кібердіалог зі Сполученими Штатами (Коваленко, 2022).

1 лютого 2022 року Президент України Володимир Зеленський підписав указ про активізацію виконання рішення РНБО «Про План реалізації Стратегії кібербезпеки України», що було ухвалене в серпні 2021 року. Стратегія на 2021 рік визначає три основні пріоритети: забезпечення безпеки кіберпростору, захист прав громадян у цифровому середовищі та інтеграція в європейський і євроатлантичний простір. Також передбачається досягнення таких ключових цілей, як реалізація прагматичного міжнародного співробітництва.

Українська Стратегія зазначає, що були враховані положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав-членів ЄС та НАТО. Однак документ не містить конкретного переліку цих положень або окремого додатку, за винятком одного з пунктів Плану реалізації, що передбачає імплементацію Директиви Європейського парламенту і Ради ЄС 2016/1148 від 6 липня 2016 року про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу як частину євроінтеграції України.

3.4. Україна в міжнародному кіберпросторі

Україна виявляє зацікавленість у підході до кібербезпеки, який відділяє Європейський Союз від інших. ЄС веде роботу в різних напрямах для гарантування кібербезпеки в Європі, включаючи забезпечення кращого Інтернету для дітей і реалізацію міжнародного співробітництва в галузі кібербезпеки та кіберзлочинності. Зростання у світі залежності різних суспільств, урядів і підприємств від Інтернету для щоденної діяльності та надання ключових послуг підкреслює критичну

важливість захисту кіберпростору від зловмисних дій, що стає ключовим пріоритетом для політиків у всьому світі (Левченко, 2021).

Постійний швидкий прогрес у сфері ІКТ, глобалізація, значне збільшення обсягів даних та зростання числа різноманітних пристроїв, які підключаються до мереж передачі даних, мають відчутний вплив на повсякденне життя, економіку та державне управління. З одного боку, розвиток ІКТ сприяє підвищенню доступності та зручності послуг, збільшенню прозорості та громадської участі в управлінні, а також зниженню витрат у державному та приватному секторах. З іншого боку, збільшення важливості технологій призводить до зростання залежності від чинних електронних рішень та підвищення очікувань щодо їх безперебійної роботи.

Протягом останніх десятиліть кібербезпека стала ключовим аспектом цифрового розвитку в Європі. Про важливість кібербезпеки свідчить створення Кіберцентру UA30 13 травня 2021 року (Левченко, 2021). Цей центр, заснований на Державній службі спеціального зв'язку та захисту інформації України, має у своєму складі Урядову команду реагування на комп'ютерні надзвичайні події України (CERT-UA). CERT-UA активно співпрацює з іншими CERT країн-членів для виявлення причин та обставин кіберінцидентів, а також для усунення загроз як для приватного, так і для іноземного секторів. Шляхом надання рекомендацій з мінімізації ризиків і технічної підтримки для подолання наслідків кібератак, CERT-UA виконує важливу роль у забезпеченні кібербезпеки в Україні та за її межами.

Закон України «Про основні засади кібербезпеки України» закріплює завдання для CERT-UA на законодавчому рівні. Згідно з цим законодавством, CERT-UA разом із Центром реагування на кіберзагрози мають забезпечувати координацію дій при відповіді на кібератаки та інциденти в режимі реального часу. Вони також відповідальні за розробку та впровадження контрзаходів, які спрямовані на зниження ризиків вразливості в системах комунікацій.

Київське відділення ISACA (Асоціації з аудиту та управління інформаційними системами) активно працює над розробкою методологій і стандартів у галузі управління, аудиту та безпеки інформаційних технологій. Ця організація об'єднує фахівців з усього світу й надає широкий спектр ресурсів для фахівців з кібербезпеки,

сприяючи керуванню та контролю над інформацією і технологіями. У різних вищих навчальних закладах України активно впроваджуються освітні програми з кібербезпеки, орієнтовані на різні рівні освіти: бакалаврський, магістерський або професійний (Левченко, 2021).

Заради підвищення міжнародного співробітництва та гармонізації нормативних документів у галузі кібербезпеки, Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність та інші міжнародні угоди відповідно до стандартів ЄС та НАТО. За сприяння трастового фонду НАТО були створені Ситуаційні центри при СБУ та ДССЗЗІ, яким доручено виявлення, запобігання та нейтралізація кібератак на Україну. Завдяки цьому в Національній поліції України діє Національний контактний пункт 24/7 для реагування та обміну інформацією про комп'ютерні злочини (Коваленко, 2022).

Для зміцнення стійкості критичної інфраструктури країни у сфері кібербезпеки, уряд України активно залучений у міжнародне співробітництво та обмін досвідом щодо реагування на кіберінциденти. Участь у міжнародних ініціативах, таких як заходи ОБСЄ, спрямовані на зміцнення довіри в кіберпросторі, а також поглиблення співпраці з ЄС та НАТО, значно підвищує потенціал України у галузі кібербезпеки і відповідає національним інтересам. Окрім того, Україна бере участь у Форумі команд реагування на інциденти інформаційної безпеки FIRST, який є міжнародною платформою для груп CERT з усієї Європи, сприяючи обміну знаннями та досвідом у цій критичній області.

Активна участь України в подібних ініціативах і співпраця з міжнародними організаціями на кшталт ОБСЄ, ЄС, та НАТО дозволяє Україні не лише зміцнювати свої кіберзахисні можливості, але й активно впливати на формування міжнародних стандартів у кібербезпеці. Таке залучення відіграє важливу роль у забезпеченні національної безпеки, сприяє технологічному розвитку та зміцнює міжнародні зв'язки. Водночас участь у глобальних кібербезпекових ініціативах стимулює Україну до подальшого розвитку власних інституціональних та технічних ресурсів, зокрема через створення і вдосконалення внутрішньодержавних структур кібербезпеки (Левченко, 2021).

Висновок до третього розділу

1. Участь України в міжнародних ініціативах свідчить про визнання важливості кібербезпеки як пріоритетного напрямку для національної та міжнародної безпеки. Зокрема, Україна активно співпрацює з міжнародними партнерами, такими як ОБСЄ, Європейський Союз та НАТО, для розробки та впровадження спільних стратегій і програм у галузі кібербезпеки. Це дозволяє країні отримувати доступ до передових технологій, стандартів і практик, а також сприяє обміну досвідом та експертизою.

2. Сучасний кіберландшафт характеризується різноманітністю та постійною зміною загроз, які можуть стати серйозними викликами для національної безпеки, економіки та суспільства загалом. Російська активність у кіберпросторі є основним викликом і загрозою для кібербезпеки України. Україна повинна активно розвивати свої кібербезпечні можливості, враховуючи широкий спектр загроз: від кібершпигунства до кібертероризму. Зокрема, для України стає критично важливим зміцнювати співпрацю з НАТО, щоб уникнути негативних наслідків від їх масового розповсюдження і виключити можливість використання таких засобів у державному та військовому секторах.

3. Стратегія кібербезпеки України визначає основні принципи й завдання для гарантування безпеки в кіберпросторі. Її цілі полягають у створенні умов для безпечного функціонування кіберпростору та захисту інтересів особи, суспільства і держави. Основні принципи стратегії включають розвиток технологій кіберзахисту, підвищення цифрової грамотності громадян, співпрацю з міжнародними партнерами та створення комплексних заходів забезпечення кібербезпеки. Головні завдання включають формування вітчизняної нормативно-правової бази у сфері кібербезпеки, створення конкурентного середовища у сфері електронних комунікацій, розвиток системи надзвичайних ситуацій та інцидентів у кіберпросторі, а також зміцнення міжнародного співробітництва.

4. Україна активно розвиває свою присутність і вплив у міжнародному кіберпросторі, акцентуючи увагу на зміцненні кібербезпеки та співпраці з глобальними партнерами. Через участь у міжнародних угодах та конвенціях, а також через взаємодію з такими організаціями, як ЄС, НАТО, та ОБСЄ, Україна покращує свої технологічні можливості та нормативно-правову базу для протидії кіберзагрозам на національному та міжнародному рівнях.

ВИСНОВКИ

1. Концепція глобального інформаційного суспільства є не лише ідеєю, але і вектором розвитку, який визначає майбутнє суспільства. Ця концепція відкриває широкі можливості для співпраці, інновацій та соціального прогресу, але водночас ставить перед собою значні виклики й ризики, пов'язані з приватністю, безпекою та доступністю інформації. Щоб досягти успіху в сучасному інформаційному віці, необхідно боротися з цими викликами на рівні національних і міжнародних стратегій, забезпечуючи баланс між відкритістю, інноваціями та безпекою.

2. Проблеми впровадження принципів правового регулювання міжнародних інформаційних відносин вимагають комплексного підходу та співпраці на міжнародному рівні. Зокрема, необхідно активізувати діалог між країнами щодо встановлення загальноприйнятих стандартів і норм, забезпечити ефективну координацію міжнародних організацій у цій сфері. Окрім цього, важливо розробити механізми для врегулювання спірних питань і вирішення правових конфліктів, що виникають у процесі впровадження таких заходів. Лише через консолідовані зусилля та взаємодію держав можна досягти успішної реалізації цих принципів і забезпечити стабільність у міжнародних інформаційних відносинах.

3. Розвиток міжнародної архітектури кібербезпеки відбувається на широкому фронті, враховуючи швидкий розвиток цифрових технологій і постійне зростання кіберзагроз. Щоразу вища важливість цифрової галузі для різних аспектів життя суспільства вимагає спільних зусиль демократичного світу на міжнародному рівні для гарантування безпеки кіберпростору. Особливу увагу слід приділяти співробітництву між державами, міжнародними організаціями та приватним сектором для створення ефективних механізмів протидії кіберзагрозам і підвищення рівня захисту в кіберпросторі.

4. Головними загрозами в українській стратегії кібербезпеки визначено гібридну агресію рф, кіберзлочинність, організовані та спонсоровані урядами недемократичних держав кібератаки, кібертероризм та інші види терористичної

діяльності. Водночас у стратегії України щодо кібербезпеки йдеться про те, що повільна імплементація положень європейського законодавства є одним із чинників, що формує вищезазначені загрози. У рамках гарантування безпеки цифрового простору Україна має спрямувати свої зусилля на розроблення національних стандартів у сфері кібербезпеки, організаційних і технічних вимог з урахуванням європейських і міжнародних стандартів.

5. Зростання кількості та якості кіберзагроз показало необхідність удосконалення національних стратегій кібербезпеки, які є частиною законодавчої функції держави. Останніми роками цифровий світ набув великого значення в застосуванні в багатьох сферах через переваги, а також через велику кількість користувачів як із державних, так і з приватних компаній. Концепція кібербезпеки була породжена постійним розвитком ІКТ через збільшення кількості користувачів, кіберзагроз і атак, а також через важливість цієї концепції як інструменту національної сили. У всьому світі кіберпростір став полем, що поширювалося на дипломатичний, інформаційний, економічний і військовий рівні глобальної та національної політики. Кібербезпека мала висхідний курс, починаючи з технічної дисципліни, розвинувшись до тактичного рівня і, нарешті, досягнувши стратегічного рівня потужних держав.

6. Кібератаки та зловмисна діяльність – це не одне й те саме, а наслідки та мотиви пов’язаної з державою транскордонної кібероперації можуть відрізнятися. Кібератаки, пов’язані з державою, визначаються як кібератаки, які призводять до травмування чи загибелі людей або пошкодження чи знищення об’єктів (DDoS-атаки чи атаки програм-вимагачів). Пов’язана ж з державою зловмисна кібердіяльність включає крадіжки інформації (шпигунство), дезінформацію та створення фальшивих вебсайтів. Зловмисна діяльність не завдає фізичної шкоди людям або об’єктам. Однак шкода у випадку шпигунства може полягати у фінансових збитках та/або підриві довіри до здатності уряду захищати конфіденційну інформацію або сіянні політичних і соціальних розбратів, таких як втручання у вибори чи референдуми в іншій країні.

7. Кіберзагрози суттєво впливають на міжнародні відносини та національну безпеку. Дедалі більша кількість кібератак та кіберінцидентів підвищує рівень напруги між державами та міжнародними організаціями, загрожуючи стабільності та безпеці у світі. Кіберзагрози можуть мати серйозні наслідки для економіки, критичної інфраструктури, політичних процесів і соціальної стабільності країн. Тому необхідно посилювати міжнародне співробітництво, розвивати механізми виявлення та протидії кіберзагрозам, а також удосконалювати національні стратегії кібербезпеки для забезпечення стійкості та захищеності суспільства від цих загроз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Антонюк, В. (2021). Інформаційна війна в структурі сучасного геополітичного протиборства: нові контексти та інтерпретації. *Державне управління: удосконалення та розвиток.* 2021. № 7. Retrieved from http://www.dy.nayka.com.ua/?op=1&z=2121

Боднар, І. (2016). Міжнародна інформація: Навчально-методичний посібник для самостійного вивчення курсу. Львів: «Новий Світ-2000»

Варламова, М. Дем'янова, Ю. (2020). Основні тенденції діджиталізації у глобальному вимірі. Галицький економічний вісник. Retrieved from http://www.economy.nayka.com.ua/?op=1&z=8525

Висоцький О.Ю. (2020). Публічна дипломатія : конспект лекцій. Дніпро : ДНУОГ,

Висоцький, О. (2017). Пропагандистські стратегії цифрової дипломатії. Освіта і наука в умовах глобальних трансформацій. СПД «Охотнік» 2017 рік: *матеріали Всеукр. наук.-практ. конф. 24-25 лист. 2017 р.* Дніпро : СПД. 9-12.

Воронкова, В. (2017). Становлення інформаційного суспільства як цивілізаційної парадигми розвитку сучасної України за доби глобалізації: теоретико-методологічні та праксеологічні виміри : монографія; ЗДІА. Запоріжжя: ЗДІА.

Гуйван, О. (2018). Міжнародно-правове регулювання інформаційних відносин. *Правові новели*. № 4. 92-99.

Глобальні тренди міжнародних відносин. Монографія. Київ : Вадекс, 2020.

Давиденко, О. (2021). Державне управління системою профілактики та протидії загрозам суспільно-політичній стабільності України: теоретичний аспект: дис. ... канд. наук з держ. упр. : 25.00.01. НАДУ. Київ.

Еннан, Р. Є. (2020). Правове регулювання відносин у мережі Інтернет. Матеріали міжнародної науково-практичної конференції ІТ-право: проблеми і перспективи розвитку в Україні. Retrieved from http://aphd.ua/publication-173/

Еллюль, Ж. (1999). Техніка, або виклик століття. Сучасна зарубіжна соціальна філософія: Хрестоматія. К.: Либідь.

Житник, О. (2021). Формування державної політики національної безпеки в умовах трансформацій у військовій сфері. Автореферат дис. … к. держ. упр. 25.00.02 – механізми державного управління. Київ: МАУП.

Запорожець, Т. (2020). Цифрова платформа інтелектуального управління у безпековій сфері. Цифрове врядування : монографія. Нац. акад. держ. упр. при Президентові України. Київ : ІДЕЯ ПРИНТ. С. 267-280

Закіров, М. (2017). Сучасні інформаційно-комунікаційні технології як фактор еволюції соціально-політичних відносин. *Наукові праці Національної бібліотеки України.* Вип.46. 11-24.

Карпчук, Н. (2018). Міжнародна інформація та суспільні комунікації: навч. посіб. Для туд. закл. вищ. освіти. Луцьк. Retrieved from https://evnuir.vnu.edu.ua/handle/123456789/14600

Кібербезпека в інформаційному суспільстві. Інформаційно-аналітичний дайджест. 2023. Retrieved from https://ippi.org.ua/sites/default/files/2023-9.pdf

Коваленко, О. (2022). Теоретико-методологічні засади формування механізмів забезпечення кібербезпеки України на сучасному етапі державного будівництва. *Věda a perspektivy*. №6 (13). 21–23.

Костенко, Д. (2021). Формування мережевої архітектури публічного управління в контексті забезпечення національної безпеки: дис. … докт. Філософії. НАДУ. Київ,.

Левченко, О. (2021). Система забезпечення інформаційної безпеки держави у воєнній сфері: основи побудови та функціонування : монографія. Житомир : Видавець ПП “Євро-Волинь”.

Лісовський, П.М. (2017). Міжнародні відносини: ментальність, геополітика, глобалізація : Навч. посіб. К.: Кондор-Видавництво.

Литвин, А. (2020). Тенденції розвитку світового ринку інформаційних технологій. Теоретичні і практичні аспекти економіки та інтелектуальної власності: збірник наукових праць. ПДТУ. Вип. 2.132-137

Піпченко, Н., Макаренко, Є., Рижков, М. (2019). Цифрова дипломатія : підруч. Київ.

Піпченко, Н., Рижков, М. (2021). Публічна дипломатія ЄС. «Принциповий прагматизм» ЄС – наслідки для Східної та Південно-Східної Європи» 2021 рік: матеріали міжнар.наук.-практ. конф., 21-22 травня. 2021 р. Київ : КНУ.

Пшетачник Я. Війна Росії проти України: хронологія кібератак [Електронний ресурс] / Я. Пшетачник, С. Тарпова ; Дослідницька служба Європейського парламенту // European Parliament. – Режим доступу : https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf.

Сагайдак, О. (2017). Дипломатичний протокол та етикет : підручник. 2-ге вид., оновл. і доповн. Київ : Знання.

Стратегічні комунікації в міжнародних відносинах: Монографія. Київ: Вадекс.

Стройко, Т. (2018). Міжнародні організації: Навч. посібник. Київ: Кондор Видавництво.

Типовий закон ЮНСІТРАЛ про електронні підписи. Законодавство України. Retrieved from https://zakon.rada.gov.ua/laws/show/995_937#Text

Указ Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Retrieved from http://zakon3.rada.gov.ua/laws/show/96/2016.

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

“Це найбільша у світі хакерська атака на телеком-інфраструктуру”. Перше інтерв’ю президента “Київстару” після кібератаки, яка паралізувала оператора. Retrieved from https://forbes.ua/innovations/pro-kiberataku-na-kiivstar-vidnovlennya-zvyazku-ta-dopomogu-microsoft-cisco-ericson-blits-intervyu-presidenta-kompanii-komarov-12122023-17855

Ченбай, Н. (2019). Трансформації ідентичності в умовах інформаційно-технологічної революції (соціокультурний аспект). *Вісник Національного авіаційного університету. Серія: Філософія. Культурологія.* Вип. 2. 95-100

Шахова, О. (2018). Роль інформаційних технологій у розвитку міжнародних відносин. Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення : зб. матеріалів доп. учасн. Міжнар. наук.-техн. конф. Тернопіль : Тернопіль.

Castells, M. The Information Age Economy, Society, and Culture. Retrieved from https://deterritorialinvestigations.files.wordpress.com/2015/03/manuel_castells_the_rise_of_the_network_societybookfi-org.pdf

Eldem T. International Cybersecurity Norms and Responsible Cyber Sovereignty. Istanbul hukuk mecmuasi. 2021. Vol. 79 (1). P. 347–378.

Kasper A., Osula A., Molnar A. EU cybersecurity and cyber diplomacy. IDP-internet law and politics. 2021. №34. P. 1–15. URL: https://raco.cat/index.php/IDP/article/view/n34-kasper/487930

Kaufmann, M., Jeandesboz, J. (2017). Politics and 'the digital': From singularity to specificity. *European Journal of Social Theory*. №20. 309–328

Makedon, V., Drobyazko, S., Shevtsova, H., Maslosh, O., Kasatkina, M. (2019). Providing security for the development of high-technology organizations, *Journal of Security and Sustainability* Issues 8(4). 1313-1331

Measuring the Information Society Report 2018. International Telecommunication Union (ITU). Retrieved from https://www.itu.int/en/ITUD/Statistics/Documents/publications/misr2018/MISR2018-Vol-2-E.pdf

Report on Information Technology (IT) 2019: Global Market Analysis from 2014 and Forecast to 2022. Retrieved from https://www.businesswire.com/news/home/20190925005479/en/2019-Report-on-Information-Technology-IT-Global-Market-Analysis-from-2014-and-Forecast-to-2022-ResearchAndMarkets.com

Shakeel N., Khan N. A framework to protect National Cyber Borders in peace and war. 16th Asia Joint Conference on Information Security (AsiaJCIS – 2021). Proceedings 16TH Asia Joint Conference on Information Security (AsiaJCIS – 2021). Seoul, 2021. P. 17–22.

Vevera A. From cyber threat to hostile action in cyberspace. Romanian journal of information technology and automatic control-revista romana de informatica si automatica. 2018. №28 (3). P. 17–30.

White, A. (2016). Manuel Castells's trilogy the information age: economy, society, and culture. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/1369118X.2016.1151066

АНОТАЦІЯ

Кваліфікаційної роботи

Тема – “Інформаційні технології в контексті міжнародних відносин: кібербезпека як один із викликів сучасної цифрової епохи”

Студент – Гринчишина Валерія Олександрівна

Рік навчання, факультет – 2024, факультет соціальних наук та соціальних технологій

Науковий керівник – Гриценко Олена Миколаївна, професор, доктор політичних наук, професор кафедри міжнародних відносин

Рецензент_____

(вчений ступінь, вчене звання, прізвище та ініціали)

Захищена “____”_____20_ р.

Короткий зміст роботи

Дипломна робота присвячена дослідженню кібербезпеки як одного з найнебезпечніших викликів сьогодення в контексті міжнародних інформаційних відносин. Окрема увага приділена таким явищам, як кібершпигунство, кібертероризм та інформаційна зброя. Зокрема, у дослідженні проаналізовані кіберзагрози на тлі повномасштабної війни рф проти України, висвітлені численні атаки на український інфопростір, застосування дипфейків та інші маніпулятивні методи впливу на маси задля підриву довіри до національних урядів, дискредитації іміджу представників держав, а також для зміни політичних орієнтацій у суспільстві. Окрім цього, у дипломній роботі наведений аналіз міжнародної співпраці для забезпечення стійкості глобального інформаційного простору та участь України в різноманітних міжнародних ініціативах для подолання транснаціональної кіберзлочинності.

Ключові слова: геополітика, глобалізація, інформаційне суспільство, інформація, кібербезпека, кіберзагрози, кіберпростір, кібертероризм, кібершпигунство, міжнародна співпраця, міжнародні відносини, національна безпека, технології.