Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин

КВАЛІФІКАЦІЙНА РОБОТА

МАГІСТРА

на тему: «**КІБЕРСУВЕРЕНІТЕТ США ЯК СКЛАДОВА НАЦІОНАЛЬНОЇ ТА ГЛОБАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**»

Виконала:
здобувачка вищої освіти 2-го курсу, групи УМІБ-61
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
ОПП «Міжнародна інформаційна безпека»
Зеленська Анастасія Олегівна

Керівник:
канд. екон. наук, доцент
Чернишова Лариса Олексіївна

Рецензент:
канд. політ. наук, доцент
Безрук Олександр Олександрович

ХАРКІВ – 2025 рік

Харківський національний університет імені В.Н.Каразіна

Навчально-науковий інститут «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Кафедра міжнародних відносин
Спеціальність 291 «Міжнародні відносини, суспільні комунікації та регіональні студії»
Освітньо-професійна програма «Міжнародна інформаційна безпека»
Рівень вищої освіти: другий (магістерський)

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ **Наталія ВІННИКОВА**
Підпис ім'я, прізвище

«02» червня 2025 року
(зі змінами від 10.09.2025; 06.10.2025)

ЗАВДАННЯ
на кваліфікаційну роботу магістра

Зеленської Анастасії Олегівни
(прізвище, ім'я та по батькові)

1. Тема роботи «Кіберсуверенітет США як складова національної та глобальної інформаційної безпеки»,
керівник роботи Чернишова Лариса Олексіївна, кандидат економічних наук, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом по університету від «02» червня 2025 р. № 4001-5/1324 зі змінами від «10» вересня 2025 року № 4001-5/3049, зі змінами від «06» жовтня 2025 року № 4001-5/3656

2. Строк подання здобувачем роботи 21 листопада 2025 р.

3. Перелік питань, які потрібно розробити:
1. Сутність поняття «інформаційна безпека» та її місце в системі національної безпеки.
2. Глобальна інформаційна безпека: сутність та підходи до забезпечення.
3. Особливості національної інформаційної безпеки США: нормативно-правова база.
4. Кіберсуверенітет як елемент національної інформаційної безпеки.
5. Формування кіберсуверенітету США: від концепції відкритого Інтернету до захисту цифрового простору.
6. Інституційне забезпечення кіберсуверенітету США.

7. Роль США у формуванні міжнародних норм і стандартів у сфері інформаційної безпеки.
8. Взаємодія США та міжнародних організацій у регулюванні кіберпростору.
9. Виклики та перспективи розвитку кіберсуверенітету США в системі глобальної інформаційної безпеки.

4. План роботи

№ з/п	Назви етапів роботи	Строк виконання етапів
1	Вибір здобувачем теми КРМ і подання заяви на кафедру; затвердження теми та призначення наукового керівника; складання та затвердження індивідуального завдання на виконання КРМ, опрацювання джерельної бази дослідження	19.05.2025-30.06.2025
2	Підготовка вступу і розділу 1 КРМ	01.09.2025-30.09.2025
3	Підготовка розділу 2 КРМ	01.10.2025-15.10.2025
4	Підготовка розділу 3 КРМ	16.10.2025-31.10.2025
5	Підготовка висновків і переліку використаних джерел	03.11.2025-14.11.2025
6	Подання здобувачем завершеної КРМ науковому керівнику для перевірки та оформлення відгуку, перевірка КРМ на відсутність запозичень	17.11.2025-21.11.2025
7	Попередній розгляд КРМ на комісії від кафедри	24.11.2025-28.11.2025
8	Доопрацювання роботи, прийняття кафедрою рішення про допуск роботи до захисту в ЕК, оформлення та зовнішнє рецензування	01.12.2025-05.12.2025
9	Підготовка до захисту та захист КРМ в ЕК і присвоєння випускникам кваліфікації	08.12.2025-23.12.2025

5. Дата видачі завдання 2 червня 2025 року (зі змінами від 10.09.2025; 06.10.2025).

Здобувач вищої освіти _____ Анастасія ЗЕЛЕНСЬКА
(підпис) (ім'я, прізвище)

Керівник роботи _____ Лариса ЧЕРНИШОВА
(підпис) (ім'я прізвище)

ЗМІСТ

ВСТУП

Актуальність теми. У цифрову епоху інформаційна безпека стала наріжним каменем національної могутності, глобальної стабільності та демократичної стійкості. Сполучені Штати, як світовий лідер у сфері технологій та політики кібербезпеки, розробили комплексний стратегічний підхід до захисту свого інформаційного простору, захисту критичної інфраструктури та сприяння безпечному, відкритому та сумісному цифровому середовищу. Стратегія США, що розвивається, відображає визнання того, що кіберпростір та цифрові технології є не лише інструментами економічного зростання та інновацій, але й сферами стратегічної конкуренції та потенційних конфліктів.

Актуальність цієї теми беззаперечна, оскільки Сполучені Штати прагнуть формувати управління, розвиток та відповідальне використання цифрових технологій через тісну співпрацю з союзниками, партнерами та суб'єктами приватного сектору. Їхня політика наголошує на «цифровій солідарності», спільному зобов'язанні побудувати стійку та поважну цифрову екосистему, яка сприяє колективній безпеці, економічній інклюзії та демократичним цінностям. У цих рамках США поєднують регуляторні ініціативи, інституційну координацію та міжнародні партнерства для боротьби з транснаціональними кіберзагрозами, просування прав людини та зміцнення глобального цифрового порядку.

Дана тематика досліджувалася різними зарубіжними та вітчизняними вченими. Серед зарубіжних вчених, які аналізували кіберсуверенітет США як складову національної та глобальної інформаційної безпеки, можна виокремити: С. Бордофф, Р. Дейберт, Е. Фішер, П. Міхаель Фішеркеллер, Б. Форка, М. Гонсалес та ін.

Вітчизняними вченими, які у своїх працях розглядали теоретичні аспекти кіберсуверенітету США як складову національної та глобальної інформаційної безпеки, були: О. Кузнецов, М. Міхровська, Т. Паламарчук, Н. Суханова, А. Левтеров та ін.

Мета та завдання роботи. Мета дослідження полягає у визначенні особливостей формування кіберсуверенітету США як складової національної та глобальної інформаційної безпеки.

Досягнення поставленої мети здійснюється вирішенням наступних завдань:

– визначити сутність національної та глобальної інформаційної безпеки;

– з’ясувати особливості нормативно-правової бази забезпечення національної інформаційної безпеки США;

– розкрити концептуальний зміст кіберсуверенітету та його місце у загальній архітектурі національної інформаційної безпеки;

– виокремити особливості становлення та інституційного забезпечення кіберсуверенітету США;

– оцінити роль США у формуванні міжнародних норм і стандартів у сфері інформаційної безпеки та розкрити їхню взаємодію з ключовими міжнародними організаціями;

– виявити основні виклики та окреслити перспективні напрями розвитку кіберсуверенітету США в сучасній системі глобальної інформаційної безпеки.

Об'єктом дослідження є система національної та глобальної інформаційної безпеки.

Предметом дослідження є кіберсуверенітет США як складова національної та глобальної інформаційної безпеки.

Теоретико-методологічна та інформаційна база дослідження. Для дослідження кіберсуверенітету як елементу цілісної системи національної безпеки та визначення особливостей правового регулювання кіберпростору США були використані такі методи, як аналіз, синтез, формалізація, порівняння, спостереження.

Для визначення ролі державних і міждержавних органів у реалізації політики інформаційної безпеки та місця кіберсуверенітету в архітектурі глобальної безпеки застосовано функціональний, системний методи,

моделювання, абстракцію, класифікацію, узагальнення. Метод структурно-функціонального аналізу дозволив оцінити взаємозалежність між елементами стратегії кіберсуверенітету США та з'ясувати логіку їх практичного функціонування. Метод інституційного аналізу застосовано для визначення ролі та взаємодії ключових федеральних агентств (DHS та CISA) у формуванні та впровадженні кіберполітики США.

Інформаційна база дослідження складалася зі складної системи міждисциплінарних джерел, що забезпечило багатовимірність, обґрунтованість та достовірність отриманих висновків. Вона включала офіційні нормативно-правові акти Сполучених Штатів у сфері інформаційної безпеки та кіберполітики, стратегічні документи Білого дому, Міністерства внутрішньої безпеки (DHS), Агентства з кібербезпеки та безпеки інфраструктури (CISA), нормативні матеріали Конгресу США, спрямовані на регулювання цифрового середовища та захист критичної інфраструктури, звіти міжнародних організацій (ООН, НАТО, ОЕСР, Міжнародного союзу електрозв'язку), академічні публікації іноземних і вітчизняних вчених, що розглядали теоретичні та методологічні підходи до інформаційної безпеки, цифрового суверенітету.

Практичне значення отриманих результатів. Результати дослідження можуть слугувати ґрунтовною основою для подальших академічних та порівняльних досліджень у сфері міжнародної кіберполітики, особливо щодо ролі основних глобальних акторів у формуванні цифрового порядку. Рекомендації, розроблені в межах дослідження, мають практичну актуальність для державних органів, відповідальних за захист інформації та критичної цифрової інфраструктури. Вони можуть бути використані для вдосконалення процесів оцінки ризиків, розробки ефективніших механізмів міжнародного співробітництва та підтримки формулювання або перегляду національних стратегічних документів у сфері кібербезпеки.

Апробація результатів дослідження була проведена на всеукраїнському Науково-практичному круглому столі «Стратегічні напрями зовнішньої

політики та дипломатії країн світу» (Харків, 21 листопада 2025 р.), тема тез доповідей: «Роль кіберсувернітету в системі національної безпеки США».

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел, що нараховує 85 найменування. Загальна кількість сторінок роботи складає 83, основна частина робити викладена на 74 сторінках.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ НАЦІОНАЛЬНОЇ ТА ГЛОБАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1. Сутність поняття «інформаційна безпека» та її місце в системі національної безпеки

Сьогодні існує багато різних визначень поняття безпеки, які ґрунтуються на різних критеріях та підходах дослідників. У деяких випадках безпека розглядається як стан стабільності, розвитку та сприятливих умов існування. Водночас надмірна орієнтація лише на збереження безпеки може обмежувати інновації та прогрес, що призводить до застою та консерватизму. Тому поняття безпеки слід розуміти не лише як захист від небезпеки, а й як умову, що забезпечує постійний розвиток при збереженні стабільності системи [18].

У сучасному розумінні безпека часто пов’язується з превенцією – здатністю зменшувати або усувати небезпеку й загрози. Термін «захист» відображає важливу функцію безпеки, проте не розкриває її повністю. Безпека також охоплює відсутність або мінімізацію ризиків, здатних завдати шкоди. Оскільки абсолютна безпека є недосяжною, її доцільно розглядати як динамічний процес управління ризиками, попередження загроз і підтримання стійкості системи.

У різних культурах поняття безпеки зазвичай пов’язується з усвідомленням людиною власного захисту від шкідливих впливів. Безпека є не лише зовнішнім станом, а також внутрішнім відчуттям впевненості та захищеності [22]. Для забезпечення такого захисту громадян, суспільства і держави кожна країна створює власну систему безпеки, яка включає як об’єкти захисту (людей, інформацію, інфраструктуру), так і суб’єкти, відповідальні за забезпечення цієї безпеки.

Етимологічно термін «безпека» означає відсутність небезпеки. Для повнішого розуміння цього поняття необхідно враховувати його протилежні категорії, а саме небезпеку та загрозу. Небезпека виникає внаслідок негативних факторів, які порушують право людини на життя і здоров’я або загрожують

існуванню та розвитку організацій. Тому поняття безпеки, ризику та небезпеки тісно пов’язані між собою та відображають необхідність попередження небажаних втрат у процесі життєдіяльності людини та функціонування суспільства.

Безпека може бути охарактеризована як здатність системи протидіяти загрозам і водночас досягати розвитку. Вона є основою існування будь-якої системи, забезпечуючи захист її цінностей, цілей і інтересів. У сучасному світі особливого значення набуває інформаційна складова безпеки. Інформація стала фундаментальним елементом суспільного, політичного та економічного життя. Наявність ризиків, пов’язаних з інформаційними процесами, створює підґрунтя для формування поняття інформаційної безпеки [73].

Інформаційна безпека описує стан захищеності інформаційного середовища особи, суспільства і держави. Вона забезпечує стабільність інформаційних процесів, надійність інформаційних систем та інфраструктур. У сучасних умовах національна безпека має виразний інформаційний вимір. Зростання значення інформаційних ресурсів, технологій та комунікаційних мереж робить інформаційну безпеку одним із пріоритетних напрямів забезпечення національної безпеки [39].

Національна безпека реалізується на двох основних рівнях, а саме на суспільному та державному. Кожен із цих рівнів має внутрішній і зовнішній аспекти залежно від джерел потенційних загроз. Особиста безпека є фундаментом національної безпеки, оскільки захист прав та інформаційної стабільності особи безпосередньо впливає на стійкість суспільства і держави.

Інформація може бути не лише засобом комунікації, а й інструментом впливу. Переконувальна або маніпулятивна інформація здатна формувати поведінку, погляди та установки людей. Такий вплив може бути як позитивним, так і негативним. Якщо інформація використовується з руйнівною метою, вона може суперечити інтересам особи чи суспільства, створюючи конфлікти та психологічну напругу. Цей вплив може бути як відкритим, так і прихованим, але в будь-якому випадку він позначається на свідомості людини.

Інформаційна безпека є складним і багатогранним явищем, що охоплює технічні, правові, соціальні та психологічні аспекти. Вона не існує без об’єкта захисту, адже безпека завжди спрямована на збереження чогось конкретного, а саме людини, організації чи системи. Основною метою інформаційної безпеки є запобігання шкоді в інформаційній сфері та захист від умисних або випадкових негативних впливів.

У контексті глобалізації інформаційна безпека забезпечує захист національних інтересів і стабільність суспільства, запобігаючи втручанню, маніпуляціям і поширенню неправдивої або деструктивної інформації. Вона гарантує функціонування державних інституцій, сприяє розвитку громадянського суспільства та підтримує довіру громадян до джерел інформації і комунікаційних систем [23].

У сучасних умовах питання захисту інформації є ключовим для будь-якої сфери людської діяльності. Захист і класифікація інформації можуть сприяти зміцненню національної безпеки та формуванню сприятливого середовища для її зберігання. Такі фактори зумовлені глобальними процесами загострення конфліктів. Тому для державної політики питання забезпечення національної безпеки є пріоритетним у контексті глобальної політичної нестабільності та необхідності врегулювання існуючих конфліктів.

Крім того, для забезпечення національної безпеки використовуються різні форми контролю доступу до інформації. Однією з найпоширеніших у сучасних умовах є трипартитний тест, який дозволяє проаналізувати реальну важливість інформації та потенційну шкоду від її розголошення.

Сутність публічної інформації в науковій літературі розглядається з кількох позицій, зокрема з правової та політичної. [16]. Питання правової природи доступу до публічної інформації є ключовим для розвитку відкритої системи економічного потенціалу та правових норм у державі. За своєю суттю публічна інформація забезпечує громадянину можливість отримати основні факти про діяльність підприємства, організації, державну політику чи стратегію.

Для формування ефективної правової бази доступу до державної інформації необхідно створити дієвий механізм доступності та класифікації. Такі аспекти мають існувати, щоб уникнути проблем, пов'язаних із розголошенням державної таємниці або ключової стратегічної інформації. Слід зазначити, що в умовах розвитку сучасних глобальних подій потреба у створенні системи інформаційної безпеки стає першочерговим завданням.

Основні сфери, які слід оптимізувати в межах обмежень доступу до публічної інформації:

– інформація про військові об'єкти та стратегію держави. Це ключовий елемент стратегічного розвитку національної безпеки. Можливість розголошення таких даних може становити загрозу для існування держави, особливо з урахуванням поточних подій у світі. Тому, незважаючи на право людини отримувати інформацію про діяльність армії, такі дані мають ретельно перевірятися щодо можливості їх публікації;

– інформація про діяльність політичних діячів і дипломатичні угоди. Головним завданням є створення режиму державної таємниці для питань, які можуть забезпечити конкурентні переваги у сфері дипломатичного та економічного розвитку країни. Водночас надання доступу до таких даних можливе лише у разі, якщо це не суперечить стратегічним інтересам держави;

– інформація про державні фінансові установи та соціально-інвестиційні організації. Прозорість діяльності таких структур є ключовим напрямом для запобігання корупції та забезпечення відкритості тендерів. У більшості країн система публічної звітності про фінансові результати компаній залишається недосконалою. Для її вдосконалення використовуються незалежні аудити, що дають об'єктивну оцінку діяльності організації [3].

Зазначені напрями становлять основу національної безпеки, оскільки саме вони є найбільш вразливими з точки зору витоку інформації [32]. Тому держава повинна розробити раціональну систему доступу до даних і забезпечити ефективну регуляторну діяльність. Саме завдяки таким

регуляторним механізмам підприємства та державні установи можуть підвищити ефективність своєї роботи.

Проблематика публічної інформації формує правову основу розвитку демократії та свободи слова. Методологія обмеження доступу до інформації є ознакою тоталітаризму й обмеження прав і свобод людини, що негативно впливає на формування демократичного суспільства [10].

У великих фінансових установах і судових органах зберігається значний обсяг інформації про діяльність компаній і реалізацію їхньої політики. Для підвищення ефективності функціонування необхідно впроваджувати політику покращення доступу до інформації. Найбільш поширеним інструментом у сучасних державах є трипартитний тест, який дозволяє визначити:

– чи можна надати доступ до певної інформації;
– чи може її розголошення зашкодити національній безпеці;
– чи містить вона дані про стратегічні або інфраструктурні об’єкти.

Використання такого підходу дозволяє точно визначити ступінь відкритості інформації та адекватно оцінити діяльність організації відповідно до її сфери функціонування.

Сьогодні важливим напрямом є підвищення прозорості діяльності організацій на основі відкритості даних. Це сприятиме розв’язанню ключових суспільних проблем, зокрема:

– подоланню корупції, шляхом забезпечення доступу громадян до даних про державні закупівлі, тендери та фінансові операції;

– удосконаленню судової системи, оскільки відкритість судових процесів підвищує незалежність правосуддя та зміцнює довіру до державних інститутів;

– захисту права на свободу слова, що забезпечує можливість журналістських розслідувань, суспільних дискусій і підвищення рівня громадського контролю;

– просуванню позитивного іміджу держави, адже відкритість і прозорість інформаційних процесів сприяють інвестиційній привабливості країни та зменшенню ризиків корупції.

Отже, інформаційна безпека є визначальною ознакою сучасної епохи. Вона відображає здатність особи, суспільства і держави захищати себе в інформаційному середовищі, протидіяти загрозам та сприяти розвитку. Забезпечення інформаційної безпеки є не лише технічним завданням, а й фундаментальною умовою сталого національного розвитку, збереження ідентичності, стабільності та суверенітету держави в цифрову епоху.

1.2. Глобальна інформаційна безпека: сутність та підходи до забезпечення

У сучасному світі організації значною мірою залежать від своїх інформаційних систем (ІС) не лише у щоденній діяльності, а й у реалізації стратегічних планів розвитку. Інформаційні системи стали невід'ємною частиною глобальної інформаційної інфраструктури, визначаючи рівень конкурентоспроможності, ефективності та стабільності як окремих підприємств, так і держав у цілому. Зростаюча залежність від цифрових технологій і віртуальних середовищ, таких як мережеві організації або віртуальні корпорації, свідчить про те, що інформаційні системи є основою сучасної глобальної економіки та управління [25].

Разом із цим посилюються і ризики. Як організації, так і їхні інформаційні системи стикаються зі зростаючою складністю, швидкими технологічними змінами та збільшенням кількості загроз. До них належать кібернапади, витоки даних, а також інформаційні кампанії з дезінформації, які часто виходять за межі державних кордонів. Тому забезпечення глобальної інформаційної безпеки потребує системного підходу, що охоплює не лише технічні, а й організаційні, управлінські та людські чинники.

Інформаційну безпеку в такому контексті можна визначити як здатність інформаційних систем зберігати свою функціональність, надійність та цілісність в умовах внутрішніх і зовнішніх ризиків. Для досягнення цього держави та організації мають забезпечити, щоб їхні інформаційні системи були здатні:

– адаптуватися до змін середовища та нових загроз;

– навчатися та розвиватися з метою управління новими викликами;

– ефективно комунікувати всередині системи та між системами для забезпечення обміну інформацією та координації.

Таким чином, інформаційна безпека стає не просто технічним завданням, а ключовою функцією стратегічного управління. Її слід інтегрувати у загальну систему менеджменту організації або держави, а не розглядати як окремий або додатковий елемент. Основним принципом має бути не лише захист інформаційних компонентів, а передусім забезпечення спроможності системи виконувати свої функції та досягати поставлених цілей.

Важливим теоретичним підґрунтям сучасного управління інформаційною безпекою є закон необхідної різноманітності Ешбі (Ashby's Law of Requisite Variety), згідно з яким лише різноманітність може контролювати різноманітність. У контексті глобальної інформаційної безпеки це означає, що механізми управління ризиками мають бути настільки ж складними та гнучкими, як і потенційні загрози. На практиці це потребує створення динамічних і адаптивних систем безпеки, які розвиваються разом із технологіями, на відміну від статичних моделей оцінки ризиків, що швидко застарівають [65].

Інформаційна безпека сьогодні розглядається не лише як технічне завдання, а як складова глобальної системи права і міжнародних відносин. Відомі приклади таких правових ініціатив: Загальний регламент про захист даних (GDPR) у Європейському Союзі, Закон про конфіденційність споживачів Каліфорнії (CCPA) у США та Акт про захист персональних даних (PDPA) у Сінгапурі. Ці нормативні акти формують правове підґрунтя для створення

безпечного цифрового середовища та встановлюють чіткі вимоги до обробки персональних даних [57].

Зокрема, GDPR став глобальним еталоном у сфері захисту даних, оскільки поширює свою дію не лише на країни ЄС, але й на будь-які компанії, які працюють із даними громадян Європи. Порушення його вимог може призвести до значних штрафів, а саме до 4% річного обороту компанії або 20 мільйонів євро. Аналогічно, CCPA у США посилив права споживачів щодо контролю над власною інформацією, а PDPA у Сінгапурі створив збалансовану систему, яка поєднує захист приватності з економічною ефективністю.

Однак, попри розвиток таких правових механізмів, глобальні виклики інформаційній безпеці залишаються надзвичайно серйозними. Хакери постійно вдосконалюють свої методи, а кількість даних, що потребують захисту, зростає експоненціально [79]. Основними загрозами сьогодні є:

– кібертероризм і міждержавні кібератаки;
– витоки персональних даних і корпоративної інформації;
– розповсюдження дезінформації та інформаційних маніпуляцій;
– недосконалість або фрагментарність правового регулювання у різних країнах.

Проблемою залишається і відсутність єдиного міжнародного підходу до забезпечення інформаційної безпеки. Наявність різних стандартів і законів ускладнює співпрацю між державами, унеможливлює ефективне переслідування кіберзлочинців та створює нерівні умови для бізнесу [63]. Тому на сучасному етапі дедалі більшої ваги набуває необхідність міжнародної координації, створення уніфікованих принципів і спільних механізмів реагування на кіберзагрози.

Розв’язання цих проблем вимагає консолідованих дій усіх учасників інформаційного простору, зокрема держав, бізнесу, експертних спільнот і звичайних користувачів. Підвищення рівня цифрової грамотності, використання сучасних засобів кіберзахисту (шифрування, брандмауери, системи моніторингу) та впровадження етичних стандартів обробки інформації

є важливими елементами побудови стійкої системи глобальної інформаційної безпеки [34].

Тим не менш, ми можемо обґрунтовано очікувати, що майбутнє кібербезпеки буде характеризуватися чотирма тенденціями, а саме:

– використання блокчейн-технологій ,

– розширення ролі штучного інтелекту ,

– залучення колективного інтелекту та посилення глобального співробітництва у сфері кібербезпеки

Сучасні блокчейн-технології є результатом десятиліть досліджень і розробок. Деякі з них (наприклад, інфраструктура Bitcoin) витримали численні кібератаки та наочно продемонстрували, що, попри децентралізований характер, їм можна довіряти. Цілі держави вирішили покладатися на блокчейн для захисту своєї інформаційної інфраструктури [84]. Так, Естонія захищає свою всесвітньо відому систему електронного урядування та високорозвинене цифрове суспільство за допомогою масштабованої блокчейн-технології, створеної у відповідь на кібератаки 2007 року [74].

Окрім державних органів, багато великих корпорацій також вирішили впроваджувати блокчейн у свої системи інформаційної безпеки. Наприклад, Lockheed Martin (американська компанія, що спеціалізується у галузях аерокосмічної, оборонної, безпекової та високих технологій) оголосила про плани використати блокчейн у своїй стратегії кібербезпеки. У цьому контексті Рон Бессір, віцепрезидент із інженерії та технічних операцій Lockheed Martin, зазначив: «Ці нові підходи до кібербезпеки підвищать цілісність даних, пришвидшать виявлення проблем і реагування на них» [57].

Блокчейн-технології є особливо корисними для захисту конфіденційних даних. Наприклад, 1 мільйон медичних записів Естонії захищено за допомогою технології блокчейн, розробленої естонською компанією Guardtime. На її основі створено інфраструктуру безключових підписів (Keyless Signature Infrastructure, KSI), яка є альтернативою традиційній інфраструктурі відкритих ключів (PKI). У 2017 році Міністерство енергетики США обрало Guardtime та низку

партнерів для розроблення блокчейн-технології кіберзахисту розподілених енергетичних ресурсів [68].

Крім захисту інформації, блокчейн може використовуватись для усунення потреби у паролях, що, у свою чергу, зменшує кількість атак соціальної інженерії, спрямованих на викрадення облікових даних [84].

Використання штучного інтелекту (Artificial Intelligence, AI) дає змогу постачальникам рішень у сфері кібербезпеки підвищувати стійкість комп'ютерної інфраструктури.

Наприклад, британська компанія Darktrace застосовує машинне навчання для аналізу нормального стану мережі та виявлення в реальному часі будь-яких аномалій у її роботі. Машинне навчання можна визначити як здатність машини навчатися без явного програмування [53].

Інша компанія «Hexadite» також успішно використовує штучний інтелект [52]. Її рішення аналізує сповіщення систем безпеки та усуває виявлені вразливості. За даними компанії, Hexadite є «першим рішенням із безперервної автоматизації реагування на кіберінциденти, що поєднує виявлення й усунення загроз» [51].

У другому десятилітті XXI століття було засновано велику кількість компаній, які спеціалізуються на AI-рішеннях для кібербезпеки, зокрема CrowdStrike (2011), Cylance (2012), Darktrace (2013), Illumio (2013), Hexadite (2014), Harvest AI (2014). Зважаючи на швидке зростання таких компаній, можна очікувати, що використання AI у кібербезпеці незабаром стане повсюдним [66].

Водночас штучний інтелект несе не лише переваги, а й потенційні ризики. Кіберзлочинці можуть створювати «розумне» шкідливе програмне забезпечення, здатне автоматично сканувати мережі на наявність вразливостей, генерувати спеціалізовані інструменти для атак і швидко поширюватися між системами.

У своєму зверненні «Про стан держави» колишній президент США Барак Обама наголосив на важливості інтеграції розвідувальних даних для боротьби з

кіберзагрозами. Проте збір і обробка великих обсягів даних потребують значних людських та фінансових ресурсів.

Краудсорсингом називають практику передавання завдань онлайн-спільноті замість традиційних постачальників послуг, що може дати змогу організаціям інтегрувати розвідувальну інформацію з кібербезпеки ефективніше та економніше.

Попри те, що наразі не існує єдиної глобальної краудсорсингової платформи для обміну даними про джерела кібератак, такі пропозиції вже з'являються. Краудсорсинг можна використовувати не лише для повідомлення про інциденти безпеки, а й для тестування кіберзахисту [44].

З кожним роком зростає кількість ініціатив щодо обміну розвідувальними даними з інформаційної безпеки між країнами та організаціями.

Хоча деякі проєкти (наприклад, спроба створити кібербезпековий підрозділ США – Росія, про який згадував Дональд Трамп) не були реалізовані, інші ініціативи мають перспективи перерости у нормативно-правові механізми. Зокрема, в ЄС триває активна дискусія щодо створення міжнародної правової бази для обміну інформацією про кіберінциденти.

Одним із успішних прикладів є SWIFT Information Sharing and Analysis Centre (SWIFT ISAC), створений у 2017 році для підвищення обізнаності учасників системи SWIFT про кіберзагрози та вдосконалення механізмів захисту від атак. Центр забезпечує доступ до порталу з інформацією про шкідливе програмне забезпечення, файлові хеші та тактики кіберзлочинців [68].

Основною перешкодою для створення міжурядового глобального центру кібербезпеки, який дозволив би державам обмінюватися розвідувальними даними, є національні обмеження у сфері захисту даних. Цю проблему можна вирішити лише на законодавчому рівні.

Деякий прогрес у цьому напрямі досягла некомерційна організація Financial Services Information Sharing and Analysis Center (FS-ISAC), яка працює над виявленням і усуненням європейських регуляторних бар'єрів, що перешкоджають міжнародному обміну інформацією у фінансовому секторі.

Почавшись як американська ініціатива, FS-ISAC перетворилася на міжнародну організацію, що активно діє в Європі, Африці та на Близькому Сході [68].

Тож, інформаційну безпеку слід розглядати як безперервний та адаптивний процес, своєрідну життєздатну систему, яка здатна підтримувати свою цілісність у мінливому середовищі. Життєздатна інформаційна система ефективно управляє ризиками як внутрішнього, так і зовнішнього походження, забезпечуючи стабільність і стійкість.

На глобальному рівні цей підхід передбачає необхідність:

– міжнародного співробітництва у розробленні адаптивних стандартів кібербезпеки;

– інтеграції управління інформаційною безпекою у стратегічне планування;

– постійної освіти та обміну знаннями для відповідності зростаючій складності кіберзагроз;

– розвитку стійких архітектур інформаційних систем, які здатні відновлюватися після атак.

Отже, глобальна інформаційна безпека є не лише захистом даних або мереж, а насамперед забезпеченням довгострокової життєздатності глобальної інформаційної екосистеми. Ефективні підходи до її забезпечення мають поєднувати технологічні рішення, управлінські практики, освітні програми та міжнародну співпрацю, що разом створюють систему, здатну адаптуватися й функціонувати в умовах динамічного та взаємопов’язаного світу.

1.3. Особливості національної інформаційної безпеки США: нормативно-правова база

Цифрові технології зараз впливають майже на кожен аспект життя у Сполучених Штатах. Відкритість та взаємозв'язок, що забезпечуються доступом до Інтернету, змінили функціонування суспільства. Ця реальність стала особливо очевидною під час пандемії COVID-19 [2]. Визнаючи це,

федеральний уряд виділив значні ресурси через Закон про двопартійну інфраструктуру, інвестувавши 65 мільярдів доларів у розширення надійного високошвидкісного доступу до Інтернету для кожного американця [76].

Оскільки цифрові технології все більше інтегруються в повсякденну діяльність, починаючи від спілкування з близькими та участі в соціальних мережах до ведення бізнесу та задоволення основних потреб, то довіра до безпеки, надійності та захищеності цифрової екосистеми стає дедалі важливішою. Національна інформаційна безпека окреслює комплексний підхід до зміцнення цієї довіри та забезпечення того, щоб Сполучені Штати були готові повною мірою скористатися перевагами свого цифрового майбутнього [6].

Кібербезпека лежить в основі майже кожного виміру сучасного життя: економіки, критичної інфраструктури, демократичних інституцій, особистої конфіденційності та національної оборони. З початку нинішньої адміністрації докладаються рішучі зусилля для зміцнення кібербезпеки шляхом дій виконавчої влади, співпраці з приватним сектором та міжнародних партнерств. Ці заходи спрямовані на захист громадян від кібератак, притягнення зловмисників до відповідальності та захист від кампаній, що загрожують національній безпеці та особистій конфіденційності [31].

Основні напрями національної інформаційної безпеки США визначено в Національній стратегії кібербезпеки. Ключовим акцентом стратегії є співпраця, особливо між державним та приватним секторами [9]. Вона визнає, що тягар кібербезпеки часто надто сильно лягає на окремих осіб та малі організації. Щоб вирішити цю проблему, стратегія прагне перебалансувати відповідальність, сприяти довгостроковим інвестиціям у безпеку та стійкість, а також стимулювати інновації в захисних технологіях. Вона також підкреслює важливість співпраці з союзниками для встановлення норм відповідальної поведінки держав у кіберпросторі та притягнення до відповідальності тих, хто діє безвідповідально.

У ширшому сенсі, цей момент є поворотним у тому, як суспільства формують своє цифрове майбутнє. Вибір, зроблений зараз, визначатиме структуру та етику Інтернету на десятиліття вперед. Головна мета полягає в тому, щоб зберегти Інтернет відкритим, глобальним, сумісним, надійним та безпечним, заснованим на універсальних правах людини та основних свободах. Цифрове підключення має розширювати можливості людей, а не слугувати інструментом репресій чи примусу.

По суті, Національна стратегія кібербезпеки позиціонує Сполучені Штати – разом зі своїми союзниками – для керування з сильної позиції та зі спільним баченням, спрямовуючи світ до більш безпечного та справедливого цифрового майбутнього [76].

У всьому світі Сполучені Штати Америки перебувають у авангарді розроблення політики та стратегії у сфері кібербезпеки. Ще у 2003 році уряд країни представив першу національну стратегію кібербезпеки – Національну стратегію забезпечення безпеки кіберпростору (National Strategy to Secure Cyberspace). Першими державами Європейського Союзу, які опублікували аналогічні документи, що стосувалися аспектів кібербезпеки, стали Німеччина (2005 рік) і Швеція (2006 рік).

Національна стратегія забезпечення безпеки кіберпростору 2003 року визначила три стратегічні цілі національної кібербезпеки:

– запобігання кібератакам на критичну інфраструктуру країни;

– зменшення національної вразливості до кібератак;

– мінімізацію шкоди та скорочення часу відновлення після кібератак, якщо вони відбуваються.

Для досягнення цих цілей було визначено п’ять національних пріоритетів: забезпечення безпеки федеральних комп’ютерних систем і мереж; розроблення системи реагування; створення програми зниження загроз і вразливостей; започаткування програми підвищення обізнаності та навчання у сфері кібербезпеки; а також розвиток системи міжнародного співробітництва.

На сьогодні політика США у сфері кібербезпеки складається з фрагментарних заходів; так само й законодавство є менш комплексним і більш тематично орієнтованим. Понад 50 законодавчих актів регулюють різні аспекти кібербезпеки. Відсутність єдиного рамкового закону або всеосяжної національної стратегії кібербезпеки, яка б об'єднувала наявні документи й комплексно описувала поточну стратегію, ускладнює формування чіткого розуміння загальних стратегічних цілей і пріоритетів у сфері кібербезпеки. Більшість чинних документів охоплюють національні пріоритети у вузьких сферах, що призводить до розбіжностей у структурі та змісті, а також не визначає, як ці документи співвідносяться між собою або замінюють один одного. Здебільшого вони не пояснюють, яким чином узгоджуються з єдиною національною стратегією кібербезпеки.

Більш широкі стратегії національної безпеки й оборони також включають цілі у сфері кібербезпеки. Національна стратегія безпеки 2010 року стала першою, що приділила значну увагу кіберзагрозам; вона також засвідчила зміну характеру сприйняття кіберзагроз федеральним урядом, оскільки акцент змістився від терористичних загроз з боку недержавних акторів до діяльності, яку підтримують держави, а також від переважно політичної до економічної проблематики. Чотирирічний огляд внутрішньої безпеки (Quadrennial Homeland Security Review) 2010 року визначив «захист і забезпечення безпеки кіберпростору» як одну з п'яти пріоритетних місій національної безпеки [19].

Для реалізації Національної стратегії безпеки та досягнення цілей, визначених у Чотирирічному огляді внутрішньої безпеки, Міністерство внутрішньої безпеки США (DHS) у 2011 році представило план дій «Blueprint for a Secure Cyber Future», який охоплював два ключові напрями: захист критичної інформаційної інфраструктури та зміцнення кіберекосистеми. Наступний огляд внутрішньої безпеки 2014 року визначив пріоритетом інвестиції, що підтримують національні інтереси й місії, зокрема у сфері кібербезпеки, і окреслив кіберзагрози, які становлять ризик для національних інтересів. У ньому було уточнено відповідальність Міністерства оборони (DoD)

за розвиток нових і розширених повномасштабних кіберспроможностей для захисту країни та підтримки військових місій у всьому світі. Чотирирічний огляд оборони (Quadrennial Defense Review) 2014 року визначив основні завдання Міністерства оборони у кіберсфері: «захищати цілісність мереж Міністерства оборони, забезпечувати безпеку ключових систем і мереж, проводити ефективні кібероперації за кордоном за відповідним дорученням і захищати державу від неминучої руйнівної кібератаки на життєво важливі інтереси США» [15].

Чинна Національна стратегія безпеки, ухвалена на початку 2015 року, визнає зростаючу небезпеку деструктивних і навіть руйнівних кібератак та відображає намір США зміцнювати кібербезпеку критичної інфраструктури, збільшувати інвестиції в кіберспроможності та «накладати витрати» на зловмисних кіберактрів. У документі особлива увага приділяється прагненню США просувати міжнародні норми поведінки у кіберпросторі. Визначені в Національній стратегії безпеки пріоритети підтримуються Національною розвідувальною стратегією Сполучених Штатів Америки (2014), яка серед чотирьох основних місій розвідувальної спільноти визначає виявлення та розуміння кіберзагроз із метою забезпечення процесу прийняття рішень у сфері національної безпеки, кіберзахисту та кібервпливу [76]. Стратегія підтверджує такі завдання, як посилення партнерств і обміну інформацією, а також розвиток технологічних спроможностей.

У 2011 році Білий дім оприлюднив Міжнародну стратегію для кіберпростору (International Strategy for Cyberspace), що відображає підхід США до взаємодії з міжнародними партнерами та визначення національних пріоритетів. Головна мета цієї стратегії сформульована так:

Сполучені Штати працюватимуть на міжнародному рівні задля просування відкритої, сумісної, безпечної та надійної інформаційно-комунікаційної інфраструктури, яка підтримує міжнародну торгівлю й комерцію, зміцнює міжнародну безпеку та сприяє свободі вираження поглядів і інноваціям.

Для досягнення цієї мети було передбачено створення й підтримання середовища, у якому норми відповідальної поведінки визначатимуть дії держав, зміцнюватимуть партнерства та забезпечуватимуть верховенство права в кіберпросторі. Стратегія поділяє цю мету на дипломатичні, оборонні та розвиткові напрями, окреслюючи пріоритети державної політики у семи взаємопов'язаних сферах діяльності: економіка, захист національних мереж, правоохоронна діяльність, військовий сектор, управління інтернетом, міжнародний розвиток і свобода інтернету [19].

Решта цього розділу містила хронологічний огляд найважливіших стратегічних документів і федерального законодавства, включно з актами Конгресу та виконавчими указами президентів США, що стосуються комплексного («whole-of-government») підходу до забезпечення кібербезпеки. Ці документи охоплювали широкий спектр питань: захист критичної національної інфраструктури та безпеку федеральних комп'ютерних систем і мереж; розподіл ролей і відповідальності між федеральними, державними, місцевими, племінними, територіальними та приватними суб'єктами; зміцнення партнерства між державним і приватним секторами; а також аспекти кібербезпеки у контексті міжнародної та національної безпеки, оборони й контррозвідки [15].

Стратегічний підхід США до захисту критичної інфраструктури (Critical Infrastructure Protection, CIP) базується на партнерстві між державним і приватним секторами, при цьому державні органи зберігають координуючі та пріоритетні повноваження. Така структура була започаткована Президентською директивою з прийняття рішень №63 (Presidential Decision Directive 63) від 1998 року, яка створила структуру під керівництвом Білого дому для координації федеральних заходів із захисту критичної інфраструктури від кібератак [3].

Закон про внутрішню безпеку (Homeland Security Act) 2002 року створив Міністерство внутрішньої безпеки США (Department of Homeland Security, DHS) та наділив його повноваженнями координувати національні зусилля у сфері захисту критичної інфраструктури в галузях інформаційних технологій і

зв’язку, перебравши більшість функцій, визначених у Національній стратегії забезпечення безпеки кіберпростору 2003 року.

Національну політику щодо ідентифікації, пріоритезації та захисту критичної інфраструктури у фізичному середовищі та кіберпросторі від терористичних загроз було закріплено у Президентській директиві з питань внутрішньої безпеки №7 (Homeland Security Presidential Directive 7, HSPD-7), ухваленій у 2003 році. Ця директива уточнила ролі та відповідальність різних агентств, підтвердила координуючу роль DHS у загальному процесі захисту критичної інфраструктури та визначила його як провідне агентство для секторів IT і комунікацій з метою забезпечення обміну інформацією про загрози, оцінювання вразливостей, а також розроблення планів дій і планів реагування на надзвичайні ситуації [54].

HSPD-7 також зобов’язала DHS розробити Національний план захисту інфраструктури (National Infrastructure Protection Plan, NIPP), який визначає принципи партнерства між федеральним урядом і власниками або операторами критичної інфраструктури. NIPP було прийнято у 2006 році та оновлено у 2009-му. Паралельно з Національною стратегією забезпечення безпеки кіберпростору у 2003 році було оприлюднено Національну стратегію фізичного захисту критичної інфраструктури та ключових об’єктів (National Strategy for the Physical Protection of Critical Infrastructures and Key Assets), у якій ідентифіковано критичні об’єкти країни та визначено загрози, що їм притаманні; основна відповідальність за їхній захист покладалася на DHS.

Після невдалих спроб Конгресу ухвалити законопроєкт, який би надав DHS повноваження щодо забезпечення кібербезпеки мереж критичної інфраструктури, адміністрація президента Обами у 2012 році видала Виконавчий указ №13636 (Executive Order 13636) – «Покращення кібербезпеки критичної інфраструктури» (Improving Critical Infrastructure Cybersecurity). Цей знаковий документ, чинний протягом президентського терміну, доповнив попередні акти, запровадив удосконалений порядок обміну інформацією між

федеральним урядом і приватним сектором та встановив мінімальні вимоги до підвищення рівня безпеки критичної інфраструктури.

Паралельно з EO 13636 було видано Президентську політичну директиву з питань безпеки та стійкості критичної інфраструктури (Presidential Policy Directive 21, PPD-21 – Critical Infrastructure Security and Resilience), яка зберегла чинну політику, ролі та відповідальність, але передбачала перегляд існуючої моделі державно-приватного партнерства, визначення базових даних і системних вимог для ефективного обміну інформацією, а також створення системи ситуаційної обізнаності. PPD-21 також вимагала оновлення версії NIPP від 2009 року, унаслідок чого третє видання документа було опубліковано у 2013 році.

Для усунення недоліків Закону про управління інформаційною безпекою на федеральному рівні (Federal Information Security Management Act, FISMA) EO 13636 зобов'язав федеральний уряд розробити добровільну рамкову систему кібербезпеки, що зрештою вилилося у створення «Рамки для покращення кібербезпеки критичної інфраструктури» (Framework for Improving Critical Infrastructure Cybersecurity) 2014 року. Ця рамка містить керівні принципи, практики та добровільні стандарти для приватного сектору, покликані допомогти організаціям започаткувати або вдосконалити програми кібербезпеки, використовуючи галузевий підхід до управління ризиками.

Окрім виконавчих документів, у 2014 році було прийнято чотири ключові закони, пов'язані із захистом критичної інфраструктури:

1. Закон про модернізацію управління інформаційною безпекою (Federal Information Security Modernization Act of 2014), який вніс зміни до FISMA 2002 року, уточнив роль DHS у забезпеченні безпеки цифрової інформації федеральних агентств, визначив відповідальність Офісу управління та бюджету (Office of Management and Budget, OMB) за реалізацію вимог FISMA на федеральному рівні та запровадив вимоги щодо звітування про кіберінциденти;

2. Закон про національний захист кібербезпеки (National Cybersecurity Protection Act of 2014), який дозволяє DHS обмінюватися інформацією з

приватним сектором, реагувати на кіберінциденти, надавати допомогу приватним компаніям і федеральним відомствам, а також рекомендувати заходи з кібербезпеки;

3. Закон про національну кібербезпеку та захист критичної інфраструктури (National Cybersecurity and Critical Infrastructure Protection Act of 2013), який закріплює роль DHS у запобіганні кіберінцидентам і реагуванні на них, а також створює партнерство з обміну інформацією між DHS і власниками або операторами критичної інфраструктури;

4. Закон про вдосконалення кібербезпеки (Cybersecurity Enhancement Act of 2014), який надає Національному інституту стандартів і технологій (National Institute of Standards and Technology, NIST) повноваження та підтримку для розроблення добровільних стандартів зниження ризику кібератак на критичну інфраструктуру.

Федеральні агентства також отримали завдання оцінити чинні нормативні акти у сфері кібербезпеки в межах своїх галузей відповідальності та, за потреби, розробити нові регуляторні стандарти. Наразі DHS, Міністерство торгівлі (Department of Commerce) та Міністерство фінансів (Department of the Treasury) розглядають пакети стимулів, покликані заохотити приватний сектор до дотримання положень Рамки з покращення кібербезпеки критичної інфраструктури.

Головне контрольно-ревізійне управління США (Government Accountability Office, GAO) яке часто називають вартовим Конгресу, звернуло увагу на нестачу чітких вказівок із питань кібербезпеки з боку федеральних департаментів та агентств щодо конкретних секторів критичної інфраструктури, за які вони відповідають [48]. Рівень обов’язковості дотримання вимог кібербезпеки, встановлених законом або регулюванням, значно варіюється між різними секторами критичної інфраструктури. Крім того, GAO зазначило брак чіткого розподілу відповідальності між державними та приватними структурами, а також між федеральними й штатними органами, попри формальне розмежування їхніх функцій.

Національна рамка реагування (National Response Framework) визначає основні принципи, що забезпечують узгоджену національну реакцію на катастрофи й надзвичайні ситуації, включно з кіберінцидентами. Документ має широку цільову аудиторію, зокрема від приватного сектору до неурядових організацій і громадян, при цьому для недержавних суб'єктів його виконання є добровільним. У ньому окреслено ролі різних організацій у процесі реагування на кризи, делеговано менші завдання керівникам департаментів, із фокусом на координації співпраці, а не на управлінні конкретними кризами.

Додаток «Cyber Incident Annex» до Рамки реагування роз'яснює взаємопов'язаність кіберзаконодавства та команд реагування. Наприклад, Національний план реагування на кіберінциденти (National Cyber Incident Response Plan), який визначає порядок оперативної координації та реалізації можливостей реагування на кіберінциденти, перебуває під керівництвом Національного центру інтеграції кібербезпеки та комунікацій (National Cybersecurity and Communications Integration Center, NCCIC) та його підрозділу US-CERT (United States Computer Emergency Readiness Team).

Отже, система національної інформаційної безпеки США є однією з найрозвиненіших у світі, що ґрунтується на поєднанні нормативно-правових актів, стратегічних документів та інституційної координації між державними й приватними структурами. Американський підхід до забезпечення інформаційної безпеки передбачає постійне оновлення законодавства відповідно до технологічних викликів, активну роль федеральних відомств (зокрема, DHS, DoD, NIST) та широке залучення приватного сектору через механізми партнерства у сфері критичної інфраструктури.

Нормативна база США у сфері кібербезпеки розвивається еволюційно, а саме від базових стратегій початку 2000-х до сучасних ініціатив, що поєднують національну безпеку, економічні інтереси та захист прав людини в цифровому середовищі. Інституційний механізм функціонує за принципом «whole-of-government approach», який передбачає координацію дій усіх рівнів влади з

міжнародними партнерами, приватними компаніями та громадянським суспільством.

Висновки до розділу 1

В епоху безпрецедентної цифрової трансформації глобальна інформаційна безпека стала наріжним каменем політичної стабільності, економічного розвитку та суспільної довіри. Зростаюча складність та взаємозалежність цифрових інфраструктур підкреслюють необхідність застосування цілісних та адаптивних підходів до кібербезпеки. Як було показано, сучасні виклики – від кібератак та витоків даних до дезінформації та порушень конфіденційності – вимагають інтеграції технологічних інновацій, міжнародної співпраці та комплексних правових баз.

Сучасні тенденції, такі як впровадження технологій блокчейн, розширення ролі штучного інтелекту, використання колективного інтелекту через краудсорсинг та зміцнення транскордонної співпраці, означають зміну парадигми від реактивного захисту до проактивної стійкості. Ці підходи разом переосмислюють принципи глобального управління кібербезпекою, підкреслюючи прозорість, підзвітність та спільну відповідальність між державами, організаціями та окремими особами.

Крім того, аналіз показує, що ефективну інформаційну безпеку не можна розглядати виключно як технічну чи організаційну проблему; це радше багатовимірне явище, яке перетинається з правом, етикою, економікою та міжнародними відносинами. Таким чином, забезпечення цілісності, конфіденційності та доступності інформаційних активів вимагає постійних інновацій, адаптивного регулювання та глобальної солідарності.

Зрештою, досягнення безпечного цифрового майбутнього залежить від нашої колективної здатності передбачати нові загрози, відповідально використовувати передові технології та сприяти культурі кіберінформованості та співпраці. Тільки завдяки постійній відданості цим принципам міжнародна

спільнота може захистити цифрову екосистему та підтримувати довіру, яка лежить в основі сучасного суспільства.

Національна система інформаційної безпеки Сполучених Штатів є однією з найсучасніших та найповніших систем у світі. Вона побудована на надійному поєднанні законодавчих заходів, стратегічних документів та інтегрованого інституційного механізму, який забезпечує ефективну координацію між федеральними агентствами, суб'єктами приватного сектору та міжнародними партнерами. Підхід США наголошує на динамічному балансі між захистом національних інтересів, сприянням інноваціям та захистом прав особистості в цифровому середовищі.

Еволюція архітектури кібербезпеки та інформаційної безпеки США від ранньої Національної стратегії безпеки кіберпростору (2003) до найновішої Національної стратегії кібербезпеки (2023) ілюструє послідовний перехід до моделі «всього уряду» та «всього нації». Цей підхід об'єднує зусилля різних зацікавлених сторін для посилення захисту критичної інфраструктури, підвищення стійкості та просування норм відповідальної поведінки в кіберпросторі.

Загалом, Сполучені Штати розробили адаптивну та перспективну систему, яка не лише зміцнює їхню національну безпеку, але й сприяє формуванню глобальних стандартів інформаційної безпеки та цифрового управління. Постійно модернізуючи свої правові та інституційні рамки, США демонструють свою відданість підтримці відкритої, безпечної та правозахисної цифрової екосистеми, здатної вирішувати складні виклики XXI століття.

РОЗДІЛ 2
КІБЕРСУВЕРНІТЕТ США В СИСТЕМІ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1. Кіберсуверенітет як елемент національної інформаційної безпеки

У сучасну епоху взаємодія та конвергенція кіберпростору та державного суверенітету стали критичними питаннями глобального значення, що впливають як на уряди, корпорації, так і на окремих осіб. Поширення витоків даних, кібератаки та кібервійни становлять відчутні та зростаючі загрози національній безпеці, економічній стабільності та політичній автономії. У цьому розділі розглядаються багатогранні взаємозв'язки між кібербезпекою та суверенітетом з метою аналізу викликів, з якими стикаються держави, захищаючи свою територіальну цілісність у дедалі більш взаємопов'язаному цифровому середовищі.

Концепція національного суверенітету постійно розвивалася у відповідь на історичні, політичні та технологічні трансформації. У сучасну цифрову епоху суверенітет обов'язково має поширюватися на кіберпростір, як на сферу, яка стала невід'ємною частиною здійснення державної влади та повноважень. Із прискоренням технологічного прогресу країни стають дедалі більш взаємопов'язаними та взаємозалежними, а цифрові інфраструктури формують основу економічних, політичних та соціальних систем. Хоча ця глобальна зв'язність надає безпрецедентні можливості для розвитку, інновацій та співпраці, вона одночасно створює нові та складні загрози, які потребують стратегічної уваги, а найголовнішою серед них є кібербезпека [13].

Такі явища, як хактивізм, цифровий вандалізм та навмисне поширення дезінформації, стали потужними інструментами, здатними підривати державну владу, порушувати критичну інфраструктуру та дестабілізувати політичний лад. Зростання цих кіберзагроз змусило уряди переглянути традиційні уявлення про суверенітет та взаємодіяти з реаліями глобальної інформаційної мережі як продовження геополітичної арени.

Таким чином, кібербезпека стала центральним стовпом стратегій національної безпеки в усьому світі. Зараз широко визнано, що кібервійна має потенціал завдавати збоїв, рівних з тими, що виникають у результаті звичайного військового конфлікту. Гучні інциденти, починаючи від державних кіберкампаній та операцій із застосуванням програм-вимагачів і закінчуючи кібершпигунством, виявили глибоку вразливість ключових суспільних систем, включаючи енергетичні мережі, фінансові установи та комунікаційні мережі [72]. Окрім безпосередніх технічних наслідків, такі атаки підривають довіру громадськості до урядових інституцій, дестабілізують економіку та в деяких випадках призводять до геополітичної напруженості. Отже, захист суверенітету в кіберпросторі перетворився з теоретичної проблеми на екзистенційний імператив для сучасних держав, що вимагає надійної інфраструктури кібербезпеки та комплексних політичних рамок.

Водночас кіберпростір ставить під сумнів самі основи традиційного суверенітету. Це безкордонне та децентралізоване середовище, яке не підлягає власності чи абсолютному контролю з боку жодної окремої держави. Такі проблеми, як юрисдикційна неоднозначність, труднощі з визначенням кібератак та відсутність загальновизнаних міжнародно-правових норм, ускладнюють ефективне управління кіберпростором. Більше того, оскільки уряди все більше покладаються на суб'єкти приватного сектору для створення, управління та захисту інформаційних інфраструктур, підзвітність та відповідальність стають розмитими. Ця взаємозалежність підкреслює необхідність спільного, багатостороннього підходу до кібербезпеки, який гармонізує національний суверенітет із суто глобальною природою цифрової сфери. По суті, глобалізація переосмислила параметри державного суверенітету, змушуючи нації знаходити складну рівновагу між автономією, співпрацею та стійкістю в кіберепоху [37].

У сучасну цифрову епоху кіберзагрози стали одним із найглибших викликів національному суверенітету, справляючи дестабілізуючий вплив на управління, економічну стабільність та безпеку. Охоплення кіберпростору розширилося далеко за межі його технічного походження, ставши ареною, де

здійснення державної влади та збереження національних інтересів все частіше оскаржуються. Суверенітет, який колись визначався територіальними кордонами та фізичним контролем, тепер поширюється на віртуальну сферу, де держави повинні захищати свої цифрові інфраструктури та інформаційні системи від низки складних загроз. Здатність пом'якшувати такі загрози стала важливою метою сучасної політики кібербезпеки та алгоритмічного проектування, особливо враховуючи продовження розвитку технологічної досконалості та глобальної взаємозв'язку. Як державні, так і недержавні суб'єкти тепер володіють кіберінструментами, здатними примусити, підривати та впливати, розмиваючи традиційні кордони, які колись окреслювали національну владу.

Серед найбільш прямих та найсерйозніших загроз державному суверенітету є кібератаки, особливо ті, що організовані державними організаціями. Атаки на урядові установи, військові мережі та сховища конфіденційних даних спрямовані на викрадання інформації, зрив операцій або зниження національного оборонного потенціалу. Кібервійна, як сучасна форма конфлікту, дозволяє державам досягати стратегічних цілей, не вдаючись до звичайного військового застосування [28]. Яскравим прикладом цього явища був інцидент зі Stuxnet 2010 року, який широко приписують державним суб'єктам, що застосували кіберзброю для саботажу ядерних об'єктів Ірану та тим самим підриву його суверенних можливостей. Аналогічно, постійні кібернаступи проти критичної інфраструктури України під час її триваючого конфлікту з Росією ілюструють здатність цифрової війни дестабілізувати держави, ставити під загрозу важливі послуги та підривати суверенний контроль. Такі інциденти чітко показують, що кіберагресія це не просто технічна небезпека, а екзистенційна загроза, яка змінює саму природу політичної влади та державної безпеки [17].

Вразливість критичної інфраструктури є ще одним гострим виміром виклику суверенітету. Сучасні суспільства залежать від взаємопов'язаних цифрових систем для управління такими важливими функціями, як розподіл

енергії, транспортування, фінансові операції та зв'язок. Кібератаки, спрямовані на ці системи, можуть мати каскадний вплив на національну економіку, громадську безпеку та управління, підриваючи здатність держави підтримувати стабільність та захищати своїх громадян. Атака програм-вимагачів на трубопровід «Колоніал» у Сполучених Штатах у 2021 році яскраво продемонструвала цю вразливість, порушивши постачання палива вздовж східного узбережжя та показавши, як один кіберінцидент може поставити під загрозу як економічну безперервність, так і національну безпеку. Такі збої оголюють крихкість критичної інфраструктури та підкреслюють нагальну потребу в комплексних заходах для зміцнення життєво важливих систем, забезпечуючи, щоб операційна цілісність залишалася наріжним каменем державного суверенітету в цифрову епоху [71].

Окрім технічної сфери кібератак, поширення дезінформації та кіберпропаганди становить не менш значні загрози національному суверенітету. Шляхом маніпуляцій платформами соціальних мереж та мережами цифрового зв'язку зловмисники можуть спотворювати публічний дискурс, посилювати поляризацію та підривати довіру до політичних інституцій. Ці операції спрямовані не лише на інформаційне середовище, а й на легітимність самого управління, оскільки вони прагнуть делегітимізувати уряди, порушити демократичні процеси та послабити соціальну згуртованість, від якої залежить державна влада. Втручання у президентські вибори в Сполучених Штатах 2016 року є яскравим прикладом того, як дезінформаційні кампанії можуть поставити під загрозу цілісність виборів та підірвати довіру громадськості до демократичних інституцій. Такі події показують нерозривний зв'язок між інформаційним суверенітетом та політичним суверенітетом, підкреслюючи необхідність захисту автентичності та надійності цифрової інформації як основи для підтримки стійкості держави [14].

Ширша концепція цифрового суверенітету, тобто здатність держави здійснювати контроль над своєю цифровою інфраструктурою, технологіями та даними, стала центральною в сучасних дискусіях про автономію та управління.

Однак зростаюча залежність від глобальних технологічних корпорацій та транснаціональних цифрових інфраструктур ускладнює здійснення цього контролю. Політика локалізації даних, спрямована на розширення національної юрисдикції над даними, часто суперечить комерційним інтересам багатонаціональних технологічних компаній, створюючи тертя між внутрішнім регулюванням та глобальною економічною інтеграцією. Крім того, вразливості в міжнародних ланцюгах поставок створюють додаткові ризики для безпеки. Поточні дебати щодо безпеки мереж 5G та інших критично важливих технологій ілюструють, як залежність від іноземних технологічних екосистем може поставити під загрозу здатність країни захищати свою кіберінфраструктуру та підтримувати стратегічну незалежність. Отже, підтримка цифрового суверенітету вимагає ретельного балансу між прагненням до національного контролю та необхідністю глобальної співпраці – рівноваги, яка визначає виклики управління цифрового століття.

Цифрова трансформація глобального суспільства переосмислила те, як держави керують, спілкуються та захищають свій суверенітет, одночасно створюючи нові вразливості, що виходять за рамки традиційних політичних рамок. Безкордонний та децентралізований характер кіберпростору в поєднанні зі швидкими темпами технологічних інновацій зробив класичні концепції суверенітету дедалі більш проникними. Глобалізація посилює цю напруженість, оскільки взаємозв'язок обмежує ступінь, до якої держави можуть здійснювати односторонній контроль над даними, комунікаційними мережами та критично важливою інфраструктурою [38]. Більше того, правові та регуляторні бази намагаються встигати за технологічними змінами, що призводить до значних прогалин у міжнародних нормах, що регулюють кіберпростір. Оскільки технологічний прогрес постійно перевершує оборонні можливості, багато держав постійно реагують на нові загрози, а не передбачають їх. Відсутність ефективної міжнародної співпраці ще більше посилює цю дилему, оскільки фрагментована національна політика та різні правові стандарти перешкоджають

колективному реагуванню на кіберінциденти та встановленню стабільного цифрового порядку.

Загалом, кібербезпека стала одночасно випробуванням і визначальним фактором сучасного суверенітету. Загрози, що виходять з кіберпростору, є багатовимірними та охоплюють не лише прямі атаки на інфраструктуру та оборонні системи, але й більш тонкі, але водночас дестабілізуючі маніпуляції інформацією та громадською думкою. Щоб зберегти суверенітет у цифрову епоху, держави повинні визнати, що влада більше не здійснюється виключно через територіальний контроль чи військову міць, а й через управління даними, алгоритмами та мережами. Тому забезпечення безпеки кіберпростору вимагає синтезу надійної технологічної оборони, адаптивних політичних рамок, етичного управління та міжнародної співпраці. В епоху, що визначається цифровою взаємозалежністю, стійкість суверенних держав залежатиме не лише від їхньої здатності захищатися від кіберзагроз, але й від їхньої здатності відповідально та кооперативно брати участь у глобальній цифровій екосистемі [55].

У контексті глобалізації концепція суверенітету стикається з безпрецедентними викликами, оскільки світ стає все більш взаємопов'язаним через обмін даними, товарами та послугами. Швидка глобалізація цифрових мереж сприяла економічному зростанню, інноваціям та глобальній комунікації; однак вона також накрила держави новими формами вразливості, які загрожують їхній здатності здійснювати незалежну владу. Транскордонні потоки даних, які є невід'ємною частиною функціонування глобальної цифрової економіки, ускладнюють здатність держави регулювати та контролювати інформацію в межах своєї юрисдикції. Юрисдикційні конфлікти часто виникають, коли дані, що генеруються громадянами, зберігаються на іноземних серверах, створюючи правові та безпекові ризики, пов'язані з несанкціонованим доступом або неправильним використанням зовнішніми суб'єктами [16]. Більше того, зростаюча концентрація контролю над критично важливою цифровою інфраструктурою в руках кількох потужних багатонаціональних технологічних

корпорацій переорієнтувала геополітичну владу від держав до приватних структур. Цей зсув не лише обмежує регуляторний вплив держави, але й ускладнює її здатність стверджувати суверенітет у кіберпросторі, де приватні платформи все частіше опосередковують громадське та політичне життя.

Правові та регуляторні аспекти кібербезпеки ще більше підкреслюють крихкість суверенітету в цифрову епоху. Незважаючи на зростання частоти та складності кіберзагроз, залишається мало комплексних правових баз, здатних ефективно регулювати кіберпростір. Держави продовжують стикатися зі значними перешкодами у визначенні та реагуванні на зловмисну кібердіяльність, оскільки чинні міжнародні закони часто не підходять для вирішення складнощів цієї швидкозмінної сфери. Проблема визначення винних – ідентифікації винних у кібератак – є особливо гострою, оскільки анонімність та транснаціональні мережі приховують відповідальність та перешкоджають підзвітності. Крім того, відсутність загальноприйнятих норм та стандартів поведінки держав у кіберпросторі призвела до фрагментарного та непослідовного підходу до управління кібербезпекою. Країни прийняли різні закони та політику, що відображають їхні різні політичні пріоритети та інтереси безпеки. Ця регуляторна неоднорідність створила правові вакууми, які кіберзлочинці та ворожі суб'єкти легко використовують, підриваючи як національні, так і міжнародні зусилля щодо підтримки суверенітету та стабільності в цифровій сфері [8].

Технологічні інновації є ще одним критичним викликом для збереження суверенітету, оскільки швидкий прогрес часто випереджає розробку ефективних механізмів захисту. Новітні технології, такі як штучний інтелект (ШІ), машинне навчання та квантові обчислення, все частіше використовуються зловмисниками для проведення високоскладних кібероперацій. Наприклад, алгоритми на основі ШІ можуть генерувати гіперцільові фішингові кампанії, здатні обходити звичайні системи безпеки, тоді як квантові обчислення мають потенціал для зламу існуючих протоколів шифрування, тим самим піддаючи конфіденційні дані та критичну інфраструктуру ризику експлуатації [81]. Ця

динаміка створює постійну асиметрію між зловмисниками та захисниками – безперервну гонку, в якій темпи інновацій часто сприяють тим, хто прагне використати вразливості, а не тим, хто намагається їх захистити. Прискорена еволюція наступальних кіберможливостей таким чином загрожує випередити здатність держав розробляти стійкі та адаптивні системи кібербезпеки, залишаючи навіть технологічно розвинені країни схильними до системних ризиків.

Взаємодія між глобалізацією та кібербезпекою переосмислила традиційні межі суверенітету. Транснаціональний характер цифрової взаємозалежності, неадекватність правових баз, прискорення темпів технологічних інновацій та відсутність злагодженої міжнародної співпраці разом створили складне та нестабільне середовище, в якому авторитет держави постійно оскаржується. Щоб зберегти суверенітет у цифрову епоху, держави повинні не лише посилювати свої оборонні та регуляторні можливості, а й брати участь у конструктивному міжнародному діалозі, спрямованому на розробку спільних принципів та механізмів кіберуправління. Сталість глобальної безпеки у XXI столітті залежатиме від здатності країн узгодити імперативи глобалізації з постійною необхідністю суверенного контролю та колективної цифрової стійкості .

2.2. Формування кіберсуверенітету США: від концепції відкритого Інтернету до захисту цифрового простору

Еволюція кіберсуверенітету США відображає глибоку трансформацію в глобальній політичній економіці Інтернету, зокрема від ліберального бачення відкритості та взаємозв'язку до ери, яка все більше визначається безпекою, контролем та державним втручанням. Протягом перших десятиліть розширення Інтернету Сполучені Штати відстоювали відкритий, безкордонний кіберпростір, керуючись переконанням, що вільний потік інформації сприятиме демократії, інноваціям та глобальному процвітанню. Ця доктрина «відкритого Інтернету»

була вкорінена в ліберальному оптимізмі періоду після Холодної війни, відображаючи ідеологічне переконання, що економічна взаємозалежність та технологічний прогрес принесуть стабільність та мир [46].

Однак, коли цифрова інфраструктура стала основою національних економік та критично важливих систем, вразливості цієї ліберальної моделі стали неминуче очевидними. Кібератаки, крадіжка інтелектуальної власності, дезінформаційні кампанії та експлуатація американських технологічних екосистем ворожими державними та недержавними суб'єктами виявили крихкість нерегульованого кіберпростору. Такі інциденти, як операція Stuxnet 2010 року, китайське кібершпигунство проти американських корпорацій та втручання Росії у президентські вибори в США 2016 року, продемонстрували, що сама відкритість, яка колись вважалася ознакою ліберальної сучасності, перетворилася на стратегічну перешкоду. У цьому контексті Сполучені Штати почали переосмислювати свій підхід, переходячи від бачення цифрової взаємозалежності до бачення, заснованого на захисті свого цифрового суверенітету.

Цей зсув породив нову політичну парадигму, яка прагнула збалансувати інновації з безпекою. Створення Кіберкомандування США у 2009 році, публікація Національної кіберстратегії у 2018 році та інтеграція кібербезпеки в захист критичної інфраструктури – все це відображає інституціоналізацію цифрового суверенітету [17] . У цих рамках суверенітет більше не означає лише контроль над фізичною територією, а поширюється на віртуальну сферу, охоплюючи управління даними, кіберзахист та технологічну автономію. Американський підхід до кіберсуверенітету, таким чином, являє собою складне узгодження між свободою та регулюванням, відкритістю та контролем – спробу зберегти переваги цифрової глобалізації, одночасно пом'якшуючи її невід'ємні ризики.

Одним із найпереконливіших проявів цієї еволюції є ринково-орієнтований шлях до національної стійкості, що втілюється в таких ініціативах, як Знак кібердовіри США (CTM). Запроваджений за часів

адміністрації Байдена, CTM являє собою добровільну систему маркування продуктів Інтернету речей (IoT), призначену для сигналізації про відповідність стандартам кібербезпеки. На відміну від нормативного регулювання, CTM діє через ринкові стимули, а не примусові мандати. Він заохочує виробників застосовувати безпечні методи проектування, водночас надаючи споживачам та корпоративним покупцям можливість приймати обґрунтовані рішення на основі ризику. Ця ініціатива переосмислює кібербезпеку не як суто технічну проблему, а як питання економічної раціональності – інтегруючи кіберризики в закупівлі, страхування та управління ланцюгами поставок [47].

CTM втілює ширшу філософську переорієнтацію в рамках кіберуправління США: переконання, що ринкові механізми, за умови належної структури, можуть посилити національну безпеку. Він стимулює підзвітність серед виробників, сприяє прозорості та підтримує появу ринку кіберстрахування, що ґрунтується на вимірюваному ризику. Вбудовуючи кібербезпеку в логіку конкуренції та споживчого вибору, CTM зміцнює цифрову стійкість, не вдаючись до жорсткого державного втручання. Цей підхід є прикладом поєднання ліберальних економічних принципів з прагматичним визнанням суверенітету в цифровій сфері, узгоджуючи динаміку ринку з імперативами національної оборони.

Однак трансформація кіберсуверенітету США не відбувається ізольовано. Вона розгортається в рамках швидкозмінного глобального порядку, в якому інші держави, такі як Європейський Союз, Китай та Індія, формулюють власні моделі цифрового суверенітету. Ці претензії, оформлені як зусилля щодо забезпечення автономії та захисту внутрішніх інтересів, відображають зростаючу конвергенцію між економічним управлінням та політикою безпеки. Напруженість між глобалізацією та суверенітетом стала визначальною рисою цифрової епохи. Хоча транскордонні потоки даних залишаються життєвою силою інновацій та торгівлі, вони також наражають країни на нові вразливості. Юрисдикційні конфлікти щодо зберігання, контролю та спостереження даних

підкреслюють складність застосування територіальних понять суверенітету до безкордонного цифрового простору [31] .

Цей ландшафт, що змінюється, також відродив дебати щодо політичної економії цифрового суверенітету. Історично склалося так, що лідерство США у просуванні ліберального, ринково-орієнтованого інтернет-порядку співіснувало зі значними державними інвестиціями в технологічні інновації. Однак, оскільки глобальна конкуренція посилюється, а концентрація цифрової влади в руках кількох транснаціональних корпорацій зростає, ліберальна модель все більше перебуває під тиском. Зростання неомеркантилістської політики в Сполучених Штатах, яка наголошує на поверненні виробництва, експортному контролі над передовими технологіями та сек'юритизації ланцюгів поставок, сигналізує про відхід від ідеалів невтручання держави 1990-х років.

Цей неомеркантилістський поворот переосмислює цифровий суверенітет через призму національної безпеки. Економічна взаємозалежність, колись визнана стабілізуючою силою, тепер часто зображується як стратегічна вразливість. Політика, що обмежує експорт напівпровідників та технологій штучного інтелекту, виправдана під гаслом «економічної безпеки», ілюструє, як цифрове управління перепліталося з геополітичним суперництвом. Твердження, що «економічна безпека – це національна безпека», кодифіковане в стратегічних документах США, відображає цей парадигматичний зсув. Це легітимізує виняткові заходи, такі як виконавчі укази та експортний контроль, під обґрунтуванням захисту суверенітету в умовах дедалі більш ворожого міжнародного середовища.

Таким чином, траєкторію кіберсуверенітету США можна розуміти як постійні переговори між ліберальною відкритістю та сек'юризованим контролем. Рання ера Інтернету характеризувалася вірою в ринково-орієнтовану глобальну взаємозалежність; нинішній момент, навпаки, визначається прагненням до автономії та стратегічного захисту. Однак навіть у рамках цього зсуву Сполучені Штати продовжують використовувати свої ліберальні основи, а саме відкритість, інновації та підприємництво, як інструменти сили. СТМ є

прикладом цього синтезу: політика, яка захищає національну безпеку не через централізоване планування, а через розширення можливостей ринку [32].

Підсумовуючи, формування кіберсуверенітету США відображає ширшу історичну еволюцію самого ліберального міжнародного порядку. Це історія про те, як ідеали цифрової відкритості зіткнулися з імперативами безпеки, що призвело до переосмислення того, що означає суверенітет у взаємозалежному, керованому даними світі. Американський досвід ілюструє, що суверенітет у двадцять першому столітті не можна просто повернути через ізоляцію чи контроль; його необхідно переосмислити шляхом ретельного узгодження технологічних інновацій, ринкових механізмів та національної стратегії

2.3. Інституційне забезпечення кіберсуверенітету США

Цифрова солідарність фундаментально вкорінена в інноваціях у відкритій, інклюзивній, безпечній та стійкій цифровій екосистемі та постійно зміцнюється ними. Хоча Сполучені Штати залишаються провідним гравцем у розвитку цифрових, критичних та нових технологій, вони визнають, що ефективний прогрес у цій галузі не може – і не повинен – досягатися ізольовано. Сталий цифровий розвиток найефективніше досягається шляхом спільної взаємодії між Сполученими Штатами, їхніми союзниками та партнерами, оскільки така співпраця сприяє колективному процвітанню, самовизначенню та стійкості. Ця взаємозалежність підкреслює стратегічне бачення, в якому спільні інновації та технологічний розвиток є основою глобальної стабільності та економічного зростання [34].

У цьому контексті Державний департамент США, у тісній координації з урядами союзників, приватним сектором та громадянським суспільством, продовжує виступати за відкриті, сумісні, безпечні, та надійні телекомунікаційні мережі, приділяючи особливу увагу розвитку та розгортанню бездротових мереж п'ятого (5G) та наступного (6G) покоління. Ці зусилля

відображають зобов'язання забезпечити, щоб цифрова інфраструктура була як технологічно надійною, так і відповідала демократичним цінностям.

Білий дім, спільно з Державним департаментом, Агентством США з міжнародного розвитку (USAID), Міністерством торгівлі та Федеральною комісією зв'язку (FCC), веде постійний діалог з міжнародними партнерами, щоб сприяти використанню перевірених постачальників у глобальному розгортанні мереж 5G та формувати майбутній розвиток технологій 6G [59].

На багатосторонньому рівні Сполучені Штати активно сприяють розвитку, розгортанню та використанню цифрових технологій з дотриманням прав людини в усіх органах Організації Об'єднаних Націй. Завдяки таким зусиллям США прагнуть інституціоналізувати принципи прозорості, підзвітності та захисту прав людини в рамках міжнародного цифрового управління.

Швидка еволюція технологій п'ятого покоління (5G) трансформувала глобальну цифрову зв'язок, створюючи як безпрецедентні можливості, так і складні вразливості кібербезпеки. Сполучені Штати виступають за те, щоб телекомунікаційні мережі будувалися з використанням продуктів від перевірених постачальників, зокрема організацій, які працюють, та чиї партнери по ланцюгу поставок працюють, у юрисдикціях, що підтримують верховенство права та незалежність судової влади, відповідно до принципів, відображених у Декларації Організації економічного співробітництва та розвитку (ОЕСР) про доступ уряду до персональних даних, що зберігаються організаціями приватного сектору. І навпаки, телекомунікаційна інфраструктура не повинна покладатися на постачальників, які перебувають під впливом або контролем авторитарних режимів, де відсутній незалежний нагляд та судові засоби захисту від втручання уряду.

Для захисту цілісності та різноманітності цифрових мереж Сполучені Штати підтримують міжнародні ініціативи, пов'язані з 5G, такі як Празькі пропозиції щодо безпеки 5G та Празькі пропозиції щодо різноманітності постачальників телекомунікацій, обидві з яких сприяють

конкурентоспроможності ринку та диверсифікації перевірених постачальників обладнання. Ці рамки зміцнюють глобальну екосистему, зменшуючи системну залежність від постачальників з високим рівнем ризику та посилюючи безпечний технологічний розвиток [76].

Відповідно до цих цілей, Сполучені Штати інтегрують свої ініціативи 5G у рамках Партнерства за глобальну інфраструктуру та інвестиції (PGII), зокрема через свій напрямок «Цифрова інфраструктура». Визнаючи, що вартість залишається домінуючим фактором у закупівлях інформаційно-комунікаційних технологій (ІКТ), Сполучені Штати підтримують національні уряди, постачальників інтернет-інфраструктури середньої милі та постачальників інтернет-послуг (ISP) у розвитку більшої конкуренції та різноманітності в ланцюгах поставок телекомунікацій. Центральним елементом цих зусиль є Партнерство з цифрового зв'язку та кібербезпеки (DCCP). Партнерство з цифрового зв'язку та кібербезпеки є загальноурядовою ініціативою,яка очолюється Державним департаментом, який забезпечує нарощування потенціалу, технічної допомоги, а також розробку та фінансування проектів для розвитку відкритого Інтернету та зміцнення глобальної кібербезпеки [79].

Подальша інституційна підтримка надається через Закон CHIPS та науку, який виділяє 500 мільйонів доларів США до Міжнародного фонду технологічної безпеки та інновацій (ITSI), що адмініструється Державним департаментом. Цей фонд забезпечує міжнародну співпрацю для розробки та впровадження безпечних ланцюгів поставок напівпровідників та телекомунікаційних мереж, що дозволяє створювати політичні та регуляторні рамки, що сприяють надійним екосистемам ІКТ та забезпечують рівні умови для безпечних постачальників [74].

Цифрова солідарність також виражається через ініціативи, що сприяють конкурентоспроможній та орієнтованій на громаду цифровій інфраструктурі. Агентство США з міжнародного розвитку (USAID), за підтримки DCCP, запустило Digital Invest, програму змішаного фінансування, розроблену для залучення приватного капіталу та зниження ризиків інвестицій у цифрову

інфраструктуру. Ця програма співпрацює з керуючими фондами та розробниками проектів для розширення підключення до Інтернету та цифрових фінансових послуг на ринках, що розвиваються. На сьогоднішній день тринадцять партнерів Digital Invest залучили 8,45 мільйона доларів початкового фінансування уряду США для мобілізації понад 300 мільйонів доларів приватних інвестицій у безпечну цифрову інфраструктуру, що згодом каталізувало 1,15 мільярда доларів додаткового фінансування від третіх сторін. Ці зусилля підкреслюють зобов'язання США розширити можливості місцевих громад та сприяти вибору споживачів, інноваціям та автономії в цифровому середовищі [79].

Програми допомоги США іноземним державам ще більше зміцнюють глобальну конкуренцію та різноманітність постачальників телекомунікацій шляхом розвитку відкритих та сумісних мережевих архітектур, зокрема через мережі відкритого радіодоступу (Open RAN). Ця архітектура полегшує вихід на ринок для нових постачальників, знижує витрати на розгортання та прискорює інновації, забезпечуючи модульне, гнучке проектування мережі. Open RAN також надає країнам, що розвиваються, можливості брати участь у глобальному ланцюжку поставок ІКТ через локальне складання та розробку програмного забезпечення. Пропонуючи надійну альтернативу залежності від ненадійних технологій, Open RAN підвищує як стійкість ланцюга поставок, так і національну безпеку. Відповідно, Державний департамент продовжує підтримувати Open RAN через комерційні випробування, техніко-економічні обґрунтування, місії зворотної торгівлі та програми навчання робочої сили.

Ці зусилля впроваджені в рамках Глобальної коаліції з телекомунікацій, створеної в жовтні 2023 року Сполученими Штатами у співпраці з Австралією, Канадою, Японією та Великою Британією, для сприяння диверсифікації ланцюгів поставок телекомунікацій та вирішення спільних проблем в управлінні цифровою інфраструктурою.

Заглядаючи в майбутнє, Сполучені Штати разом зі своїми партнерами готуються до нової ери бездротових інновацій шляхом розвитку технологій

шостого покоління (6G). Очікується, що протягом наступного десятиліття 6G забезпечить безпрецедентну швидкість підключення, розширену ємність та мінімальну затримку. Інтеграція відкритих та сумісних архітектур, таких як Open RAN, на ранніх етапах досліджень та розгортання 6G матиме вирішальне значення для забезпечення різноманітності постачальників та стійкості ланцюгів поставок. У лютому 2024 року Сполучені Штати – разом з Австралією, Канадою, Чеською Республікою, Фінляндією, Францією, Японією, Республікою Корея, Швецією та Великою Британією – схвалили спільні принципи досліджень та розробок 6G, зміцнюючи спільне бачення безпечної та справедливої еволюції зв'язку наступного покоління [71].

Оскільки передова телекомунікаційна інфраструктура формує основу глобальної цифрової економіки, її ефективність та стійкість дедалі більше залежать від безпеки та надійності ширшої інформаційної екосистеми. Поширення підключених пристроїв та експоненціальне зростання трафіку даних вимагають не лише безпечних мереж, але й надійних систем для зберігання, обробки та управління даними. У цьому контексті Сполучені Штати розширюють свою відданість цифровій солідарності за межі мережевої архітектури, обравши управління хмарними обчисленнями, центрами обробки даних та пов'язаними з ними технологіями цифрової інфраструктури. Цей комплексний підхід відображає визнання того, що майбутнє зв'язку невіддільне від цілісності, сумісності та надійності цифрового середовища, яке його підтримує.

Більше того, цифрова дипломатія США виходить за рамки бездротових інновацій. Державний департамент у партнерстві з іншими федеральними агентствами координує дії з союзниками для зміцнення розробки, розгортання та безпеки цифрової інфраструктури, включаючи системи хмарних обчислень, центри обробки даних, підводні кабелі зв'язку та супутникові мережі. Цей комплексний підхід відображає розуміння того, що цілісність та безпека глобального цифрового середовища залежать від стійкості його базової технічної архітектури.

Хмарні обчислення стали критичним фактором цифрової трансформації, забезпечуючи масштабовані та економічно ефективні обчислювальні ресурси, що лежать в основі модернізації як державного, так і приватного секторів. Завдяки надійним та адаптивним хмарним сервісам уряди та підприємства підвищують свою кіберстійкість та здатність надавати безпечні та ефективні послуги. Стратегічне значення хмарної інфраструктури стало особливо очевидним під час військової агресії Російської Федерації проти України, коли міграція урядових даних до хмарних систем зберегла важливу інформацію та забезпечила безперервність економічних та урядових операцій, незважаючи на фізичне знищення вітчизняних центрів обробки даних [73].

Підсумовуючи, стратегія США щодо цифрової солідарності та інновацій втілює кооперативну, ціннісно-орієнтовану модель глобального цифрового управління. Сприяючи партнерству, яке наголошує на відкритості, довірі та спільному технологічному прогресі, Сполучені Штати прагнуть зміцнити цифровий порядок, який є одночасно технічно безпечним та нормативно ґрунтується на демократичних принципах.

Висновки до розділу 2

Еволюція кіберсуверенітету знаменує собою одну з найглибших трансформацій у концепції та здійсненні державної влади у XXI столітті. Оскільки цифрові технології стали невід'ємною частиною економічної, політичної та військової інфраструктури, суверенітет поширився за межі територіального контролю, охоплюючи кіберпростір, критичну інфраструктуру, дані та технологічні можливості. Цей зсув відображає визнання того, що кіберпростір є як сферою можливостей, так і сферою стратегічної вразливості, де державна влада може бути оскаржена та переосмислена. Сполучені Штати пропонують переконливий приклад цієї трансформації, еволюціонувавши від головного прихильника відкритого, глобально взаємопов'язаного Інтернету до держави, яка активно інституціоналізує механізми захисту та управління своєю

цифровою сферою. На початку цифрової ери політика США ґрунтувалася на ліберальних інтернаціоналістських принципах, що підкреслювали вільний потік інформації, інновації та транскордонний обмін як шляхи до процвітання та розширення демократії. Такі ініціативи, як Інформаційна супермагістраль адміністрації Клінтона та масштабні федеральні інвестиції в цифрову інфраструктуру, посилили переконання, що відкритість та взаємозалежність генеруватимуть як економічні, так і геополітичні дивіденди. Роль держави в рамках цієї парадигми була переважно сприяючою, забезпечення стабільності, безпеки та передбачуваності для приватних підприємств і транснаціональних акторів, які рухають технологічний прогрес.

Однак, оскільки кіберпростір став глибоко переплетеним з національною безпекою та критичною інфраструктурою, вразливість цієї ліберальної моделі стала очевидною. Такі інциденти, як операція Stuxnet, широкомасштабне китайське кібершпигунство та втручання Росії у вибори в США 2016 року, продемонстрували, що необмежене цифрове підключення може наражати держави на стратегічні, економічні та демократичні ризики. Таким чином, кібербезпека стала не просто технічним питанням, а ключовим виміром суверенітету. У відповідь Сполучені Штати поступово переорієнтували свою цифрову стратегію на захист, стійкість та контроль, створивши законодавчу та інституційну базу, яка підтвердила суверенну владу в цифровій сфері.

Гібридний характер кіберсуверенітету США додатково ілюструється ринково-орієнтованими інструментами, такими як Знак кібердовіри (CTM). Ця ініціатива інтегрує добровільне дотримання вимог та стимули для споживачів у ширшу екосистему безпеки, узгоджуючи поведінку приватного сектору з національними цілями. Використовуючи економічні механізми разом з регуляторними повноваженнями, Сполучені Штати сприяють підзвітності та стійкості, зберігаючи інновації та динамізм ринку. Таким чином, американський кіберсуверенітет не є суто примусовим; він діє через розподілене управління та стратегічну мобілізацію державних, корпоративних та цивільних суб'єктів.

РОЗДІЛ 3
КІБЕРСУВЕРНІТЕТ США ЯК ЧИННИК ФОРМУВАННЯ ГЛОБАЛЬНОЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Роль США у формуванні міжнародних норм і стандартів у сфері інформаційної безпеки

Цифрова інфраструктура швидко стала основою сучасного процвітання, підтримуючи розвинені економіки, динамічні дослідницькі екосистеми, боєздатні війська, прозоре управління та відкриті суспільства. Більше ніж будь-коли раніше, інформаційні технології сприяють транснаціональній комунікації та забезпечують глобальний обіг товарів, послуг та ідей. Ці соціальні, економічні та політичні зв'язки стали незамінними для сучасного життя. Критично важливі системи, що підтримують повсякденне існування – електро- та водопостачання, управління повітряним рухом, фінансові мережі – тепер значною мірою залежать від взаємопов'язаних інформаційних платформ. Уряди все частіше використовують цифрові інструменти для оптимізації основних послуг через ініціативи електронного урядування, тоді як соціальні та політичні рухи залежать від Інтернету для організації, мобілізації та розширення свого охоплення. Мережеві технології стали повсюдними та глобальними; для кожної країни цифрова інфраструктура перетворилася – або незабаром перетвориться – на стратегічний національний актив.

Повна реалізація перспектив цифрової епохи вимагає, щоб ці системи працювали безпечно, надійно та послідовно. Люди та установи повинні бути впевнені, що інформація буде переміщена до місця призначення без перешкод чи спотворень. Забезпечення вільного потоку даних, захист конфіденційності та цілісність взаємопов’язаних мереж зараз є основоположними для американського – і глобального – економічного процвітання, національної безпеки та просування універсальних прав.

Оскільки майже третина населення світу перебуває в Інтернеті, а ще мільярди людей перебувають під впливом цифрових технологій у своєму повсякденному житті, масштаби сучасної інформаційної екосистеми є

безпрецедентними. На відміну від середини 20-го століття, коли глобальний цифровий зв’язок був відсутній, ми зараз переживаємо унікальний історичний момент, коли міжнародна спільнота може або зміцнити успіхи кіберпростору, або дозволити його вразливостям множитися. Щоб цифрові технології продовжували розширювати можливості людей, зміцнювати суспільства та стимулювати інновації, необхідні для сучасної економіки, кіберпростір повинен зберігати відкритість та сумісність, які дозволили його надзвичайне розширення. Ці характеристики базуються на надійних технічних стандартах та ефективних механізмах управління, які заслуговують на колективну підтримку. Одночасно мережі повинні залишатися безпечними та стійкими – здатними зберігати довіру користувачів та протистояти довільним, випадковим або зловмисним порушенням.

Уся світова спільнота повинна визнати виклики, що створюються зловмисними суб'єктами, що діють у кіберпросторі, та відповідно адаптувати національну та міжнародну політику. Дії в цифровій сфері дедалі частіше мають наслідки у фізичному світі. Щоб запобігти тому, щоб ризики перебування в Інтернеті затьмарювали його переваги, держави повинні працювати разом над створенням міцнішої системи верховенства права для кіберпростору. Майбутнє відкритого, сумісного, безпечного та надійного цифрового середовища залежить від здатності світу захищати те, що має витримати, протистоячи тим, хто прагне дестабілізувати або експлуатувати наші взаємопов'язані системи.

Міжнародна стратегія Сполучених Штатів у кіберпросторі ґрунтується на переконанні, що мережеві технології мають величезний потенціал – як для країни, так і для світової спільноти. Протягом останніх кількох десятиліть Сполучені Штати стали свідками того, як ці технології трансформують їхню економіку, змінюють управління та переосмислюють повсякденне життя. Однак розквіт кіберпростору також уможливив перенесення давніх офлайн-проблем – експлуатації, примусу та агресії – у цифрову сферу. Адаптуючись до цих викликів, Сполучені Штати прагнуть подавати приклад. Їхня міжнародна

політика у кіберпросторі спрямована на розширення можливостей інновацій, зміцнення глобального добробуту та підтримку принципів, що є важливими як для зовнішньої політики США, так і для майбутнього самого Інтернету [7].

Сполучені Штати також залишаються відданими захисту та розширенню переваг, які цифрові мережі приносять суспільствам та економікам усього світу.

Ці переваги мають далекосяжні наслідки. Для окремих осіб мережеві технології підвищили продуктивність, розширили можливості та допомогли подолати ізоляцію, об'єднавши людей, розділених географічним розташуванням, мовою, інвалідністю чи рідкісними захворюваннями. Для громад цифрові інструменти прискорили реагування на надзвичайні ситуації, покращили обмін інформацією для запобігання злочинності, викрили корупцію та створили нові форми політичної участі. Бізнес отримав доступ до світових ринків та абсолютно нових галузей промисловості. Уряди досягли покращень у прозорості, ефективності та залученні громадськості. На міжнародному рівні цифрові мережі сприяли формуванню глобального ринку ідей та сприяли вражаючим колективним діям під час гуманітарних криз. Чим вільніший потік інформації, тим стійкішими та активнішими стають суспільства. Тому Сполучені Штати продовжують працювати над розширенням доступу до цифрових технологій та посиленням їхньої діяльності всередині країни та за кордоном [18].

Сполучені Штати також визнають, що швидке розширення глобальних мереж створює значні ризики для національної, економічної та міжнародної безпеки. Ці виклики мають різні форми. Технічні збої або навмисний саботаж можуть порушити фізичну комунікаційну інфраструктуру. Погано розроблені методи блокування контенту в одній країні можуть ненавмисно призвести до каскадних міжнародних перебоїв. Кіберздирництво, шахрайство, крадіжка особистих даних та експлуатація дітей підривають довіру громадськості до онлайн-комерції, соціальної взаємодії та навіть особистої безпеки. Масштабна крадіжка інтелектуальної власності загрожує національній

конкурентоспроможності та підриває інновації, які її рухають [10]. Ці виклики виходять за межі кордонів: низькі бар'єри для входу в кіберпростір та легкість анонімної онлайн-активності створюють «безпечні притулки» для кіберзлочинців, іноді за мовчазної або явної державної підтримки. Більше того, кіберзагрози дедалі більше загрожують глобальному миру та стабільності, оскільки традиційні форми конфлікту поширюються в цифрову сферу.

Центральним виміром впливу Сполучених Штатів на еволюцію міжнародних норм і стандартів в інформаційній безпеці є їхні послідовні зусилля щодо закріплення глобального цифрового управління в наборі основних демократичних принципів. Вашингтон позиціонує кіберпростір не лише як технологічну сферу, а й як політичне та правове середовище, яке має відображати цінності, що є основоположними для ліберального міжнародного порядку: свободу слова, захист конфіденційності, вільний потік інформації та верховенство права. Ці принципи формують те, як США будують свою міжнародну політику щодо кіберпростору та, у свою чергу, як вони спрямовують розвиток глобальних стандартів [15]:

1. Основні свободи як нормативна база глобального кіберпростору.

Сполучені Штати стверджують, що основні свободи, зокрема свобода слова та свобода об'єднань, повинні повністю поширюватися на цифрову сферу. Ця нормативна позиція позиціонує США як провідного прихильника Інтернету, де люди можуть «шукати, отримувати та поширювати інформацію та ідеї будь-яким способом та незалежно від кордонів» [7].

Формуючи міжнародні норми, США наполягають на тому, що обмеження на онлайн-слова повинні бути винятковими, вузько спланованими та виправданими лише загальновизнаними незаконними діями, такими як експлуатація дітей, підбурювання до неминучого насильства або організація тероризму. Найголовніше, що Вашингтон розглядає ці заборони не як обмеження цінності Інтернету, а як цілеспрямовані правові відповіді на конкретні загрози [63].

Завдяки дипломатичній взаємодії, а саме в Організації Об'єднаних Націй, ОБСЄ, НАТО чи багатосторонніх коаліціях з цифрових прав американське тлумачення онлайн-свобод суттєво почало впливати на глобальні очікування щодо того, як держави повинні регулювати цифровий контент, зберігаючи при цьому демократичну відкритість;

2. Захист та безпека конфіденційності: «Збалансований підхід» як глобальний стандарт.

Другий стовп нормативного впливу США полягає у формулюванні моделі, яка узгоджує права особистої конфіденційності з імперативами національної безпеки. Згідно з американським баченням, громадяни повинні мати чітке розуміння того, як використовуються їхні персональні дані, та впевненість у тому, що вони обробляються законно та прозоро. Водночас правоохоронні органи повинні мати ефективні інструменти розслідування – під судовим наглядом – для боротьби з кіберзлочинністю, експлуатацією та іншими цифровими збитками.

Цей «збалансований підхід» став орієнтиром у міжнародних дебатах щодо управління даними, договорів про кіберзлочинність та систем спостереження. США наголошують, що механізми безпеки повинні зміцнювати, а не применшувати громадянські свободи, а гарантії конфіденційності повинні співіснувати з надійними механізмами переслідування злочинців в Інтернеті.

Вбудовуючи цю подвійну систему в міжнародні політичні дискусії, Сполучені Штати значною мірою формують глобальний консенсус щодо того, що конфіденційність та безпека взаємопідсилюють, а не взаємовиключають одне одного [41];

3. Вільний потік інформації як основа відкритого глобального цифрового порядку.

Сполучені Штати пропагують принцип, що держави не повинні бути змушені вибирати між кібербезпекою та безперешкодним потоком інформації. З точки зору Вашингтона, найефективніші рішення безпеки є адаптивними,

динамічними та мінімально нав'язливими – інструментами, які захищають системи, не підриваючи інновації, не придушуючи свободу слова та не фрагментуючи глобальну сумісність.

На противагу цьому, США розглядають національні фільтри контенту, контрольовані державою брандмаузери, примусову локалізацію даних та інші обмежувальні механізми як стратегії, що створюють «ілюзію безпеки», водночас завдаючи шкоди відкритості та економічному потенціалу глобального Інтернету. За допомогою двосторонніх та багатосторонніх ініціатив США просувають стандарти, що захищають як кібербезпеку, так і світову торгівлю, гарантуючи, що кіберпростір залишається рівним полем гри, яке винагороджує інновації, а не нав'язані державою переваги [57].

Це нормативне лідерство вплинуло на переговори щодо угод про цифрову торгівлю, міжнародних технічних стандартів та управління транскордонними потоками даних, закріплюючи ідею про те, що відкритість та безпека повинні співіснувати;

4. Верховенство права як основа міжнародної кіберстабільності.

Американський підхід позиціонує верховенство права як невід'ємну частину впорядкованого та безпечного глобального цифрового середовища. Згідно з баченням США, кіберпростір не є правовим вакуумом, бо дії в цифровій сфері повинні відповідати тим самим принципам, що регулюють поведінку у фізичному світі. Це включає:

– відповідальність держави за кіберактивність, що відбувається з її території;

– дотримання міжнародного гуманітарного права та міжнародного права прав людини;

– механізми відповідальності для зловмисних дій;

– передбачувані правові рамки, що сприяють міжнародній стабільності.

Це бачення безпосередньо впливає на внесок США в процеси ООН, такі як Генеральна група ООН та Робоча група відкритого доступу, де Вашингтон виступає за норми відповідальної поведінки держав, включаючи невтручання у

критичну інфраструктуру, співпрацю у боротьбі з кіберзлочинністю та прозору практику атрибуції.

Завдяки цим зусиллям Сполучені Штати допомагають консолідувати глобальне розуміння того, що кібероперації повинні регулюватися, бути підзвітними та відповідати встановленому міжнародному праву, тим самим стабілізуючи міжнародне середовище безпеки.

Отже, грунтуючись у своїй міжнародній політиці в кіберпросторі на фундаментальних свободах, захисті конфіденційності, вільному потоку інформації та верховенстві права, Сполучені Штати позиціонують себе як підприємця норм, що формує глобальну архітектуру інформаційної безпеки. Ці принципи слугують не лише основою внутрішньої політики, але й дипломатичними інструментами, за допомогою яких Вашингтон впливає на міжнародні стандарти, рамки управління та багатосторонні кібернорми.

Просуваючи відкрите, сумісне, безпечне та правозахисне цифрове середовище, США продовжують відігравати вирішальну роль у визначенні контурів міжнародного режиму інформаційної безпеки. Їхнє нормативне лідерство сприяє глобальному порядку, де безпека, інновації та права людини можуть співіснувати — порядку, який дедалі більше оскаржується, але все ще глибоко формується американським баченням та залученістю.

3.2. Взаємодія США та міжнародних організацій у регулюванні кіберпростору

Як держава, глибоко вкорінена в цифровій сфері, Сполучені Штати повинні мати можливість протистояти кіберзагрозам як на внутрішньому, так і на міжнародному рівні. Стратегічне значення цих загроз продовжує зростати, зумовлене ворожими суб'єктами, які все частіше використовують кібероперації для заподіяння порушень, примусу та матеріальної шкоди. Така діяльність непропорційно наражає на небезпеку цивільне населення та може надати зловмисним суб'єктам можливість прагнути дестабілізації як самоцілі. Це

піднімає центральне питання: який стратегічний підхід повинні застосувати Сполучені Штати для пом'якшення найбільш серйозних кіберзагроз. Вирішення цього питання вимагає аналізу балансу між оборонними та наступальними кіберпозиціями, оцінки їхньої відносної ефективності та оцінки того, якою мірою міжнародне право та багатосторонні інституції можуть суттєво обмежувати зловмисну кіберповедінку.

Перш ніж звернутися до зовнішньої політики США або до міжнародного кіберправа, що розвивається, саме середовище безпеки вимагає ретельної оцінки. Спектр сучасних кіберзагроз надзвичайно широкий, настільки, що вичерпне дослідження могло б стати цілим дослідницьким проектом. Загрози проявляються як на внутрішньому, так і на міжнародному рівнях, часто одночасно, через суттєво транскордонний характер кіберпростору. Для цілей цієї роботи достатньо короткого, але цілеспрямованого огляду, який підкреслює ті характеристики, що найбільше стосуються зовнішньої політики США та розвитку міжнародного права.

Кіберзагрози охоплюють широкий спектр від злочинної діяльності окремих осіб до складних наступальних операцій, що спонсоруються державою. Мотивація дуже різна, а стратегічні наслідки суттєво відрізняються; тому ефективне формування політики вимагає концептуальної диференціації. Різниця між кіберзлочинністю та кібервійною ілюструє цю потребу.

Кіберзлочинність загалом розуміється як незаконна експлуатація комп'ютерних систем недержавними суб'єктами, зазвичай мотивована економічною вигодою [21]. Широта цього визначення охоплює широкий спектр незаконної діяльності та значно ускладнює правове середовище, коли злочинці діють через національні кордони. Наприклад, атака програми-вимагача, розпочата проти критичної інфраструктури США, може випливати або з фінансово мотивованої злочинної групи, або з суб'єкта, що спонсорується державою. У першому випадку шкідливі наслідки є випадковими для прибутку; в другому випадку дія може являти собою стратегічну операцію, що наближається до порогу збройного конфлікту.

Кібервійна, навпаки, залишається концептуально суперечливою в міжнародній спільноті. Зазвичай вона стосується кібердій, спрямованих на порушення, погіршення, заперечення або знищення інформаційних систем чи мереж [83]. Ці операції за своєю суттю є стратегічними та зазвичай виконуються державними або військовими організаціями. Їхні наслідки є глибокими: держави-суперники можуть використовувати кіберможливості для шпигунства, дезінформації, крадіжки інтелектуальної власності, фізичного саботажу або атак на критичну інфраструктуру. Хоча багато держав мають наступальні кіберможливості, Китай, Іран та Північна Корея залишаються найважливішими супротивниками з точки зору розвідувального співтовариства США. Таким чином, атрибуція, що є точним визначення того, хто здійснив атаку і чому, стає нагальним пріоритетом національної безпеки.

Постійною закономірністю для всіх суб'єктів загроз є використання ними нових технологій та вразливостей для максимізації впливу за мінімальних витрат. Наприклад, нещодавний аналіз інцидентів показав, що іранські групи дедалі частіше розгортають руйнівне шкідливе програмне забезпечення, Китай вдається до масштабного використання вразливостей для отримання початкового доступу, а російські суб'єкти атакують інфраструктуру хмарних сервісів. Оскільки кіберінциденти можуть швидко призвести як до внутрішніх, так і до міжнародних наслідків, Сполучені Штати повинні підтримувати надійну та адаптивну позицію безпеки. Більше того, глобальний характер кіберпростору зумовив необхідність появи міжнародних правових баз, спрямованих на пом'якшення цих ризиків [35].

Розвиток міжнародного права у кіберпросторі є суперечливим. Тривають розбіжності щодо того, чи потрібні нові правові режими, чи можна достатньо адаптувати існуюче міжнародне право . Один табір, що складається з Китаю та кількох союзних держав, виступає за договірне регулювання кіберпростору, аналогічне механізмам контролю над озброєннями, що регулюють зброю масового знищення. Протилежний табір, очолюваний Сполученими Штатами та Європейським Союзом, стверджує, що чинне міжнародне право є

адекватним, але потребує тлумачення та вдосконалення, щоб врахувати особливий характер кібероперацій.

Незважаючи на ці суперечливі позиції, обидві сторони визнають, що кіберзлочинність та кібератаки мають за своєю суттю міжнародні наслідки. Це визнання спонукало до спроб інтегрувати кіберпитання у національні правові системи та активізувало зусилля щодо формулювання спільних кібернорм та стандартів.

Тим не менш, критики стверджують, що міжнародна спільнота розробила відносно мало обов'язкових до виконання нормативних актів, які мають реальну суттєву цінність. Лише два важливі правові документи широко згадуються як такі, що застосовуються через кордони: Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності, статті 14 та 29 якої зобов'язують держави навчати правоохоронні органи та допомагати у боротьбі з транснаціональною кіберзлочинністю; та Конвенція Ради Європи про кіберзлочинність, що супроводжується Додатковим протоколом про расистські та ксенофобські дії в Інтернеті. Останній зобов'язує підписантів криміналізувати зловживання мережами та співпрацювати у транскордонних розслідуваннях. Разом ці договори є значним прогресом, але суттєві правові невизначеності та нормативні прогалини залишаються [73].

Однією з головних спроб систематизувати застосовні міжнародні правила є Талліннський посібник з міжнародного права, що застосовується до кібероперацій. Розроблений юридичними та технічними експертами під егідою Центру передового досвіду НАТО з кооперативного кіберзахисту, посібник служить найповнішим науковим викладом того, як чинне міжнародне право застосовується як у мирному, так і в воєнному кіберконтексті. Хоча він не є юридично обов'язковим і не відображає універсальний консенсус, він має значну нормативну вагу, оскільки його автори прагнули авторитетно та послідовно тлумачити міжнародне право (2020). Таким чином, Талліннський посібник забезпечує цінну основу для роз'яснення правових неоднозначностей,

інформування державної практики та підтримки розробки більш узгоджених глобальних кібернорм [23].

Міжнародні інституції – це формалізовані домовленості, укладені між державами та іншими суб'єктами для регулювання, авторизації або обмеження поведінки в рамках глобальної системи. Тенденції в міжнародних відносинах дедалі більше вимагають скоординованого втручання через національні та організаційні кордони, особливо в таких сферах, як кіберпростір, де вразливості можуть мати далекосяжні наслідки. Поширення кіберінцидентів підкреслило ризики, пов'язані з фрагментованими або неповними системами кібербезпеки, спонукаючи держави співпрацювати через інституційні механізми для посилення як національної, так і колективної безпеки.

Інституційний ландшафт, що регулює кібербезпеку, є обширним та багатогранним, охоплюючи національні агентства, міжнародні органи та організації приватного сектору. Багато з цих організацій мають дублюючі мандати або розсіяні обов'язки, що може ускладнити координацію та підзвітність. Хоча комплексний огляд усіх інституцій у цій екосистемі виходить за рамки цього обговорення, кілька організацій є прикладами стратегічної ролі міжнародних інституцій в кіберуправлінні.

Одна з найвизначніших ініціатив виникла в рамках Організації Північноатлантичного договору (НАТО) після скоординованої серії кібератак на Естонію, члена НАТО, у 2007 році. У відповідь НАТО створило Центр передового досвіду спільної кіберзахисту (CCDCOE). Цей центр відповідає за навчання держав-членів, проведення багатонаціональних кібернавчань та підтримку операцій НАТО у разі транскордонного кіберінциденту. Хоча CCDCOE надав критично важливі ресурси кільком європейським союзникам, участь залишається добровільною, і деякі члени НАТО продовжують покладатися переважно на національні структури кіберзахисту, а не на колективну структуру.

Ще однією важливою установою є Міжнародний союз електрозв'язку (ITU) [42]. Спочатку йому було доручено стандартизувати глобальні

телекомунікації, але ITU розширив свій мандат, включивши до нього моніторинг глобального підключення до Інтернету, надання законодавчих рекомендацій та підвищення обізнаності про кібербезпеку. Він підтримує такі ініціативи, як створення національних груп реагування на комп'ютерні надзвичайні ситуації (CERT), та розробляє ресурси для допомоги державам-членам у боротьбі з кіберзлочинністю. Зовсім недавно МСЕ започаткував Глобальний порядок денний кібербезпеки (GCA), який співпрацює з Міжнародним багатостороннім партнерством проти кіберзагроз (IMPACT). IMPACT функціонує як глобальний центр реагування, сприяючи системам раннього попередження, спільному використанню ресурсів та скоординованим реагуванням на кібертероризм та загрози критичній інфраструктурі.

У сукупності ці установи ілюструють, як міжнародна співпраця може підвищити стійкість національних та глобальних мереж. Однак ефективність таких органів залишається залежною від широкої участі, чітких мандатів та інтеграції технічного, правового та стратегічного досвіду в різних юрисдикціях. У цьому контексті міжнародні установи служать не лише механізмами оперативної координації, але й нормативними платформами, формуючи очікування щодо поведінки держав та просуваючи стандарти, що підтримують глобальне управління кібербезпекою.

Хоча для боротьби з кіберзагрозами було створено міжнародне право та інституції, такі як Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності та Конвенція Ради Європи про кіберзлочинність, досі існують аргументи щодо їхньої незастосовності всередині країни, хоча й успішної з точки зору самого створення [16].

Інші колаборації, такі як Талліннська рамкова угода, не є офіційним законодавчим актом, але заявлено про амбітність у створенні базового орієнтиру для майбутніх законів.

Укладачі цієї конкретної рамки, CCDCOE НАТО, можуть фактично продемонструвати деякі проблеми застосування міжнародного права до кібербезпеки. Замість того, щоб бути членами CCDCOE, члени НАТО воліють

захищати власні мережі на національному рівні, Сполучені Штати також підходять до кібербезпеки таким чином.

Отже, у всіх своїх політичних документах щодо безпеки всі президентські адміністрації визначають кібербезпеку як проблему, яка вимагає співпраці між приватним та державним секторами. Загалом, співпраця також необхідна на міжнародному рівні, щоб повністю зробити міжнародне право основою для побудови правових баз. На даний момент у межах держав кіберзагрози, схоже, більше захищені на внутрішньому рівні.

3.3. Виклики та перспективи розвитку кіберсуверенітету США в системі глобальної інформаційної безпеки

Кібератаки здатні порушувати важливі суспільні функції з безпрецедентною швидкістю. Майже всі критично важливі послуги, включаючи роботу робочих місць, транспортні мережі, фінансові та енергетичні системи, а також комунікаційну інфраструктуру, залежать від цифрових середовищ, які залишаються дуже вразливими до складних зловживань. Успішне вторгнення в електромережу може призвести до відключення електроенергії для мільйонів людей під час суворих погодних явищ; порушення роботи транспортних мереж може зупинити мобільність у цілих мегаполісах; порушення фінансових установ може призвести до масштабних крадіжок, розкриття персональних даних та нестабільності ринку; а одночасне порушення роботи систем зв'язку може позбавити громадськість доступу до екстрених служб.

Частота, складність та операційний вплив зловмисної кібердіяльності, спрямованої проти федерального уряду та критичної інфраструктури країни, продовжують посилюватися. Нещодавня оцінка WatchBlog, заснована на оновленому Управлінням підзвітності уряду (GAO) визначенні високого ризику для федеральної кібербезпеки, висвітлює чотири головні проблеми, які продовжують підривати здатність Сполучених Штатів захищати свою цифрову екосистему [77].

Кіберсуверенітет США у системі глобальної інформаційної безпеки має наступні виклики:

1. Національній стратегії кібербезпеки бракує достатньої операційної чіткості.

Нещодавно прийнята Білим домом Національна стратегія кібербезпеки спрямована на усунення давніх структурних недоліків. Однак стратегія ще не містить показників ефективності, заснованих на результатах, необхідних для оцінки прогресу. За відсутності таких показників федеральні органи не можуть визначити, чи стратегічні ініціативи забезпечують заплановані покращення безпеки.

Крім того, федеральний уряд повинен прискорити зусилля щодо захисту глобальних ланцюгів поставок, розвитку та утримання висококваліфікованих кадрів у сфері кібербезпеки, а також управління ризиками, пов'язаними зі швидкорозвиваючимися технологіями, включаючи штучний інтелект. Наслідки недостатніх дій ілюструє компрометація SolarWinds 2019 року, в якій пов'язані з Росією суб'єкти використали широко використовувану платформу управління мережею для здійснення одного з найбільш значних вторгнень у системи уряду США та приватного сектору на сьогоднішній день. GAO видало майже 400 рекомендацій щодо посилення федеральної стратегії та нагляду за кібербезпекою, станом на травень 170 з них залишаються невиконаними [78];

2. Федеральні агентства продовжують стикатися із системними недоліками в забезпеченні безпеки систем і даних.

Федеральні агентства підтримують розгалужені інформаційні системи, які зберігають дуже конфіденційні дані платників податків, включаючи номери соціального страхування, документи про доходи, податкові декларації та інформацію про федеральні позики. Слабкі, застарілі або непослідовно впроваджені засоби контролю безпеки підвищують ризик несанкціонованого доступу та перешкоджають швидкому реагуванню на кризові ситуації.

Вразливість «Log4j», виявлена наприкінці 2021 року, підкреслює ці системні недоліки. Хоча несправний програмний компонент був вбудований у

мільйони систем з 2013 року, критична вразливість залишалася невиявленою протягом восьми років. Незважаючи на значні зусилля щодо пом'якшення наслідків, «Log4j» зараз вважається «ендемічною вразливістю», яка, ймовірно, зберігатиметься роками через її глибоку інтеграцію в державну та приватну цифрову інфраструктуру;

3. Сектори критичної інфраструктури залишаються недостатньо захищеними від ескалації кіберзагроз.

Атака програм-вимагачів на Change Healthcare продемонструвала крихкість 16 визначених секторів критичної інфраструктури країни. Інцидент порушив систему медичного виставлення рахунків по всій країні, спричинив фінансові збитки приблизно на 874 мільйони доларів, затримав надання основних медичних послуг та обмежив доступ пацієнтів до ліків.

Вразливості поширюються на всі основні сектори, а сама на енергетику, транспорт, виробництво та інші сектори, які залежать від складних, взаємопов'язаних цифрових систем, що надають широкі можливості для експлуатації. Хоча федеральні агентства розпочали зусилля щодо покращення кібербезпеки в цих секторах, залишаються значні прогалини. До них належать:

– агентства, що контролюють чотири сектори і зазнали майже половини всіх атак програм-вимагачів, не оцінили, чи відповідають їхні превентивні заходи усталеним передовим практикам;

– постійні проблеми продовжують перешкоджати координації з Агентством з кібербезпеки та безпеки інфраструктури (CISA), особливо у сферах обміну інформацією про загрози та впровадження стратегій зменшення ризиків [15];

– зацікавлені сторони на державному, місцевому та приватному рівнях повідомляють про постійні труднощі в доступі до федеральної підтримки, необхідної для усунення критичних вразливостей;

– зі 126 рекомендацій GAO, спрямованих на посилення кібербезпеки в критично важливих секторах інфраструктури, 64 залишаються невирішеними;

4. Федеральні зусилля щодо захисту особистої конфіденційності залишаються недостатніми.

У березні AT&T повідомила про витік даних, який розкрив конфіденційну особисту інформацію, включаючи номери соціального страхування та паролі, що вплинуло на понад 73 мільйони нинішніх та колишніх клієнтів. Такі інциденти зростають за масштабами та частотою, проте можливості федерального уряду запобігати, виявляти та реагувати на серйозні порушення конфіденційності залишаються обмеженими [4].

Поширення персональних та поведінкових даних, зібраних приватними компаніями, посилює ці проблеми. Багато фірм зараз створюють детальні профілі споживачів, які впливають на оцінку фінансової кредитоспроможності, можливості працевлаштування, право на страхування та досвід цифрових користувачів. Незважаючи на цю екосистему даних, що розширюється, у Сполучених Штатах відсутній комплексний федеральний закон про конфіденційність, який регулює збір, використання та поширення особистої інформації, залишаючи споживачів без послідовного правового захисту.

Навіть федеральні сховища конфіденційних персональних даних демонструють помітні недоліки. Наприклад, у 2023 році було виявлено, що IRS не має комплексного переліку систем, що містять інформацію про платників податків, що серйозно обмежує її здатність виявляти неправомірний доступ та захищати записи.

GAO видала майже 250 рекомендацій, спрямованих на вдосконалення федеральних систем захисту конфіденційності та даних; 112 рекомендацій ще не виконано.

Наведені приклади з IRS та велика кількість невиконаних рекомендацій GAO (112) яскраво демонструють, що навіть на внутрішньому, федеральному рівні Сполучені Штати стикаються із серйозними прогалинами в базовому управлінні та захисті конфіденційної інформації платників податків. Ці проблеми недоліків внутрішнього контролю та відсутності комплексних переліків систем є критичним викликом для національної безпеки.

Саме ці внутрішні слабкості стають точкою входу для зовнішніх ворогів і прямо підривають здатність держави до самозахисту у кіберпросторі.

Таким чином, для досягнення амбітної мети кіберсуверенітету – здатності держави ефективно захищати свої ключові цифрові активи та юрисдикцію – необхідно усунути ці фундаментальні внутрішні недоліки.

Це підводить нас до необхідності розгляду стратегічного підходу США до вирішення як внутрішніх, так і зовнішніх кіберзагроз.

Наведені факти щодо структурних недоліків у федеральних системах зберігання конфіденційних даних, зокрема, вразливості в інформаційних ресурсах IRS та наявність понад сотні невиконаних рекомендацій GAO, окреслюють центральний парадокс сучасної кіберполітики США. Попри глобальне технологічне лідерство, державний сектор продовжує демонструвати системні провали у сфері внутрішнього контролю, управління життєвим циклом даних та забезпечення цілісності критично важливої інформації. Такі недоліки формують фундаментальну вразливість, яка не лише знижує ефективність реагування на кібератаки, але й підриває здатність держави реалізовувати власний кіберсуверенітет.

Ці внутрішні диспропорції мають прямий стратегічний вимір: жодна держава не може успішно протистояти зовнішнім загрозам, якщо її внутрішня інфраструктура є фрагментованою, застарілою або не підкріпленою належними механізмами аудиту, відповідальності та превентивного контролю. Таким чином, внутрішня нестійкість стає не просто технічною проблемою, а чинником, який визначає межі національної могутності у цифрову епоху.

Саме з метою подолання цього подвійного виклику, поєднання необхідності структурного реформування внутрішніх кіберможливостей та потреби протистояти зростаючим зовнішньополітичним і геостратегічним загрозам, Сполучені Штати розробили комплексну багаторівневу стратегію кіберсуверенітету, яка інтегрує ключові елементи стратегічної політики США у сфері кібербезпеки (табл. 3.1).

Таблиця 3.1

Основні перспективи забезпечення кіберсувернітету США

Категорія	Перспектива/Можливість	Виклик/Загроза
1.Управління та Законодавство		
Стратегічна база	Наявність чіткої Національної стратегії кібербезпеки (наприклад, 2023 року), що вимагає від технологічних компаній більшої відповідальності за безпеку своїх продуктів (безпека за замовчуванням).	Бюрократичні та регуляторні перешкоди та політичні розбіжності, що можуть сповільнювати імплементацію стратегій.
Юрисдикція та норми	Просування міжнародних норм відповідальної поведінки в кіберпросторі та співпраця з союзниками для встановлення глобальних стандартів.	Конкуренція з іншими кібердержавами (наприклад, Китай), який просуває альтернативну, більш державно-центричну модель кіберсуверенітету
2.Технології та Інновації		
Лідерство у технологіях	Інвестування у технології (Квантові обчислення, Штучний інтелект (ШІ)) для захисту і розробки стійких систем.)	Вразливості ланцюгів постачання (Supply Chain Vulnerabilities)
Захист інфраструктури	Розробка стійких мереж, здатних відновлюватися після атак	Стрімкий розвиток кіберзагроз, та зростаюча складність критичної інфраструктури (енергетика, фінанси). I
3.Співпраця		
Партнерство	Посилення співпраці між державним сектором (CISA) та приватним сектором для обміну розвідданими про загрози	Необхідність балансу між національною безпекою та приватністю даних громадян
Міжнародні союзи	Зміцнення альянсів (НАТО) для колективної кібероборони, обміну досвідом та спільного протистояння	Необхідність уніфікації кіберпротоколів та стандартів з міжнародними партнерами, що може бути складним через різницю в законодавстві.

Таблиця багаторівневої стратегії кіберсуверенітету США репрезентована трьома взаємопов’язаними стовпами: політика, технології, партнерство. Кожен із цих стовпів не є автономним, навпаки, вони утворюють взаємозалежну

архітектуру, де політичні інструменти визначають нормативне поле, технологічні рішення забезпечують операційну дієздатність, а партнерство, як внутрішнє, так і міжнародне, що створює умови для колективної стійкості [5, 7].

Представлена таблиця деталізує ключові перспективи, можливості та стратегічні виклики, що визначають траєкторію США на шляху до утвердження повного контролю, адаптивності та довгострокової стійкості у цифровому середовищі. Саме ці фактори формують основу сучасної американської моделі кіберсуверенітету, що поєднує внутрішню модернізацію та проактивну глобальну взаємодію [20].

Отже, виклики кібербезпеці, з якими стикається уряд Сполучених Штатів, є багатогранними, динамічними та дедалі важливішими. Пом'якшення цих ризиків вимагає проактивних, скоординованих та стратегічно стійких зусиль, які поєднують розробку потужної політики, цілеспрямовані технологічні інновації, суворий регуляторний нагляд та постійне розширення кіберпраці країни. Посилена співпраця між федеральними агентствами, партнерами приватного сектору та міжнародними союзниками залишається важливою для створення стійкої та адаптивної архітектури кібербезпеки.

Надаючи пріоритет довгостроковим інвестиціям у кібербезпеку, інституціоналізуючи управління, що враховує ризики, та культивуючи культуру постійної пильності, уряд США може значно посилити свою здатність захищати інтереси національної безпеки, захищати критичну інфраструктуру та зміцнювати довіру громадськості до цілісності цифрових систем.

Висновки до розділу 3

Сполучені Штати давно позиціонують себе як центрального архітектора у формуванні сучасного режиму управління глобальним кіберпростором. Ґрунтуючись на принципах фундаментальних свобод, захисту конфіденційності, вільного потоку інформації та верховенства права,

кіберполітика США є як нормативною основою для внутрішніх стратегічних дій, так і рамкою, за допомогою якої Вашингтон формує міжнародний дискурс. Ці основні цінності дозволяють Сполученим Штатам здійснювати значний вплив на розробку глобальних стандартів, механізмів інституційного управління та багатосторонніх норм, що регулюють поведінку держав у кіберпросторі.

Просуваючи бачення відкритого, сумісного, безпечного та дотримуючогося прав цифрового середовища, Сполучені Штати продовжують відігравати провідну роль у визначенні контурів міжнародної архітектури інформаційної безпеки. Хоча геополітичне суперництво загострилося, особливо оскільки держави, які пропагують моделі суворого цифрового суверенітету та експансивного урядового контролю, прагнуть перекалібрувати глобальну динаміку влади, американське регуляторне лідерство зберігає значну нормативну силу. Воно залишається інструментом у сприянні цифровому порядку, де інновації, фундаментальні права та національна та міжнародна безпека концептуалізуються не як взаємовиключні імперативи, а як взаємозалежні компоненти узгодженої стратегічної парадигми.

Послідовні президентські адміністрації постійно наголошували на тому, що захист кіберпростору вимагає глибокої та постійної координації між державними та приватними зацікавленими сторонами. Водночас, активна міжнародна співпраця визнається важливою для створення комплексних правових та операційних рамок, здатних протистояти швидкозмінним транснаціональним кіберзагрозам. Хоча багато оборонних заходів впроваджуються у внутрішній сфері, стійка міжнародна співпраця є необхідною для формування гармонізованої та стійкої глобальної екосистеми кіберпростору.

Виклики кібербезпеці, з якими стикаються Сполучені Штати, за своєю суттю є багатогранними, динамічними та дедалі складнішими. Їх ефективне пом'якшення вимагає проактивного та стратегічно інтегрованого підходу, що охоплює вдосконалення регуляторних інструментів, розгортання інноваційних

технологічних можливостей, зміцнення механізмів нагляду, систематичне розширення національних кіберкомпетентностей та поглиблення альянсів та партнерств. Завдяки постійним інвестиціям у кібербезпеку, інституціоналізації моделей управління на основі ризиків та культивуванні культури постійної пильності, Сполучені Штати посилюють свою здатність захищати інтереси національної безпеки, забезпечувати безпеку критичної інфраструктури та підтримувати довіру громадськості до цілісності та стійкості цифрових систем.

Разом ці заходи зміцнюють статус Сполучених Штатів як вирішального та стійкого архітектора нового глобального цифрового порядку — порядку, в якому безпека, технологічний прогрес та захист прав людини стратегічно та інституційно переплетені.

ВИСНОВКИ

На основі дослідження процесу формування та розвитку кіберсуверенітету США як складової національної та глобальної інформаційної безпеки були отримані наступні результати:

1. Визначення сутності та забезпечення національної, глобальної інформаційної безпеки дозволило сформувати цілісне уявлення про здатність окремих осіб, суспільств та держав захищати себе у дедалі складнішому інформаційному середовищі, протидіяти загрозам, що розвиваються, та підтримувати довгостроковий розвиток. Інформаційна безпека охоплює набагато більше, ніж просто технічний захист: вона є фундаментальною передумовою національної стійкості, збереження ідентичності, інституційної стабільності та підтримки суверенітету в цифрову епоху. Оскільки характер ризиків змінюється залежно від контексту та обставин, вчені часто концептуалізують загрози як прояв або підвищену ймовірність конкретних ризиків, підкреслюючи багатогранний та динамічний характер інформаційних викликів. У цьому відношенні інформаційну загрозу можна розуміти як конфігурацію умов та факторів, що загрожують життєво важливим інтересам окремих осіб, суспільства та держави в інформаційній сфері.

З цієї точки зору, інформаційну безпеку слід розглядати як безперервний, адаптивний та системний процес, який нагадує життєздатну систему, здатну підтримувати внутрішню цілісність в умовах зовнішньої волатильності. Така система ефективно керує ризиками як екзогенного, так і ендогенного походження, забезпечуючи структурну стабільність, операційну безперервність та стратегічну стійкість. На глобальному рівні ця концептуалізація вимагає посилення міжнародної співпраці, інтеграції управління інформаційною безпекою в довгострокове стратегічне планування, інституціоналізації безперервної освіти та обміну знаннями, а також розробки стійких інформаційних архітектур, здатних протистояти складним формам порушень та відновлюватися після них. Глобальна інформаційна безпека – це не просто

захист даних чи мереж, а забезпечення довгострокової життєздатності та адаптивності міжнародної інформаційної екосистеми.

2. Дослідження особливостей нормативно-правової бази національної інформаційної безпеки США показало, що ця держава розробила одну з найповніших та інституційно зрілих систем національної інформаційної безпеки. Ґрунтуючись на постійно зростаючому корпусі нормативних актів, стратегічних рамок та багаторівневій інституційній координації між державними органами та приватними зацікавленими сторонами, американська модель демонструє особливу здатність до адаптації до технологічних, геополітичних та суспільних викликів. Законодавство США у сфері кібербезпеки поступово розвивалося – від основоположних стратегічних документів початку 2000-х років до сучасних ініціатив, які одночасно стосуються пріоритетів національної безпеки, економічної конкурентоспроможності та захисту прав людини в цифровій сфері. Інституційна архітектура, що функціонує за загальноурядовою парадигмою, забезпечує скоординовану взаємодію між федеральними, державними та місцевими суб'єктами у тісній співпраці з приватними підприємствами, громадянським суспільством та міжнародними союзниками.

3. Розглядаючи концептуальний зміст кіберсуверенітету та його місце у загальній архітектурі національної інформаційної безпеки, було визначено, що концепція його формування набуває нових смислових вимірів, де контроль над цифровими інфраструктурами та інформаційними потоками стає невід’ємною складовою безпеки держави. Кіберсуверенітет відображає здатність держави не лише захищати власні критично важливі системи, інформаційні ресурси та дані, а й формувати політичну, правову та технологічну рамку для протидії кіберзагрозам. Він є стратегічним інструментом збереження національної автономії в умовах глобальної цифрової взаємозалежності, забезпечуючи державі можливість здійснювати ефективне управління, захист економічної стабільності, безпеку громадян та стратегічних інтересів.

Кіберсуверенітет є ключовим елементом національної інформаційної безпеки, оскільки він інтегрує технічні, організаційні та політичні механізми для запобігання дестабілізації державних структур через кібератаки, цифрову дезінформацію та інші форми гібридних загроз. Він вимагає комплексного підходу, який поєднує національні зусилля з міжнародним співробітництвом, враховуючи безкордонний та децентралізований характер цифрового середовища. У цьому сенсі кіберсуверенітет стає не лише гарантією національної безпеки, а й фундаментом політичної стабільності, довіри суспільства до державних інституцій та здатності держави зберігати свою автономію у все більш взаємопов'язаному світі.

4. Оцінка становлення та інституційного забезпечення кіберсуверенітету США ілюструє одну з найважливіших трансформацій державної влади у XXI столітті. Оскільки цифрові технології глибоко впроваджуються в економічну, політичну та військову інфраструктуру, суверенітет поширився за межі територіальних кордонів, охоплюючи кіберпростір, цифрову інфраструктуру, управління даними та технологічні можливості. Спочатку заснований на ліберальних інтернаціоналістських принципах, які наголошують на відкритості, інноваціях та транскордонних інформаційних потоках, підхід США поступово змінювався у відповідь на нові вразливості. Стратегічні потрясіння, такі як Stuxnet, масштабне кібершпигунство та іноземне втручання в демократичні процеси, підкреслили крихкість нерегульованої цифрової взаємозалежності. Як наслідок, Сполучені Штати дедалі більше інституціоналізували механізми, спрямовані на захист та управління своєю цифровою сферою, включаючи знакові законодавчі акти (Закон про обмін інформацією про кібербезпеку, Закон CLOUD), ключові виконавчі укази та створення спеціалізованих агенцій, таких як Кіберкомандування США, Агенцію з кібербезпеки та безпеки інфраструктури та Офіс Національного директора з кібербезпеки.

Гібридна модель кіберсуверенітету США поєднує регуляторні повноваження з ринково-орієнтованими інструментами, прикладом яких є Знак кібердовіри (CTM), які узгоджують стимули приватного сектору з цілями

національної безпеки, зберігаючи при цьому інновації та економічний динамізм.

5. Визначення ролі США у формуванні міжнародних норм і стандартів у сфері інформаційної безпеки та їхньої взаємодії з міжнародними організаціями у регулюванні кіберпростору показало, що на міжнародній арені кіберсуверенітет став центральним елементом глобальної інформаційної безпеки, оскільки держави все частіше стикаються з транснаціональними викликами, такими як програми-вимагачі, дезінформація та системні ризики для взаємопов'язаних інфраструктур. Безкордонний характер цифрових мереж ускладнює традиційні уявлення про суверенітет, що вимагає адаптивних стратегій, які інтегрують право, технології, дипломатію та багатостороннє управління. На цьому тлі Сполучені Штати зміцнили свою роль головного архітектора глобального режиму управління кіберпростором. Ґрунтуючись на принципах основоположних свобод, захисту конфіденційності, вільного потоку інформації та верховенства права, кіберполітика США забезпечує як нормативну основу для внутрішньої стратегії, так і рамки, що формують міжнародний дискурс. Відстоюючи відкрите, сумісне, безпечне та засноване на правах цифрове середовище, Сполучені Штати здійснюють тривалий нормативний вплив на глобальні стандарти, механізми інституційного управління та багатосторонні кібернорми. Хоча геополітична конкуренція посилюється, особливо з боку держав, які виступають за обмежувальні, орієнтовані на суверенітет цифрові моделі, американське лідерство у співпраці з міжнародними організаціями залишається ключовим у просуванні цифрового порядку, де інновації, права людини та безпека функціонують як взаємопідсилюючі стовпи.

6. Досліджуючи основні виклики та перспективні напрями розвитку кіберсуверенітету США в системі глобальної інформаційної безпеки, було виявлено активну роботу держави щодо зміцнення кіберсуверенітету та прийняття проактивних, скоординованих та стратегічно інтегрованих рішень, що охоплюють удосконалення нормативного регулювання, технологічні

інновації, посилений нагляд та глибші міжнародні партнерства. Завдяки постійним інвестиціям у кібербезпеку, управління на основі ризиків та культивування культури пильності, Сполучені Штати зміцнюють свою здатність захищати національну безпеку, захищати критичну інфраструктуру та підтримувати довіру громадськості до цілісності цифрових систем. Разом ці зусилля зміцнюють позицію Сполучених Штатів як рішучого та стійкого архітектора глобального цифрового порядку, що формується, такого, в якому безпека, технологічний прогрес та захист прав людини інституційно взаємопов'язані та стратегічно нероздільні.

США дедалі чіткіше усвідомлюють, що національна безпека в цифрову епоху визначається не стільки здатністю створювати інновації, скільки спроможністю забезпечити їхній захист, прозорість управління та підзвітність усіх суб'єктів кіберпростору. У цьому контексті три стовпи, зокрема політика, технології та партнерство, функціонують як інтегрована система, де кожен компонент підсилює інший. Політичні механізми забезпечують нормативну визначеність і стратегічну передбачуваність; технологічні інновації формують операційну стійкість та швидкість реагування; партнерства, а саме міжвідомчі, та міжнародні, створюють умови для колективного протистояння транснаціональним кіберзагрозам.

Таким чином, американська модель кіберсуверенітету постає не як статична конструкція, а як динамічна стратегічна екосистема, здатна адаптуватися до швидкоплинних глобальних умов. Її ефективність залежить від здатності держави послідовно усувати внутрішні інституційні прогалини, впроваджувати передові технологічні рішення та будувати довгострокові партнерські альянси. Саме на цьому перетині внутрішньої модернізації, технологічної інновації та міжнародної взаємодії формується потенціал США зберігати й зміцнювати свій кіберсуверенітет у все більш складному та конфліктному цифровому середовищі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кузнецов О. Кібербезпека в епоху штучного інтелекту. URL: https://doi.org/10.52058/3041-1793-2024-4(4)-341-346 (дата звернення: 23.10.2025).

2. Міхровська М. Діджитизація, діджиталізація, цифрова трансформація: зміст та особливості. *Грааль науки*. 2021. №1 URL: https://doi.org/10.36074/grail-of-science.19.02.2021.023 (дата звернення: 17.09.2025).

3. Паламарчук Т. Artificial intelligence governance regulation in public administration. Наукові інновації та передові технології. 2024. No. 3(31). URL: https://doi.org/10.52058/2786-5274-2024-3(31)-73-81 (дата звернення: 17.04.2024).

4. Плехова Г., Суханова Н., Левтеров А. Кібербезпека: загрози, рішення. С. 681–692. URL: https://doi.org/10.46299/isg.2022.mono.econ.2.9.6 (дата звернення: 22.10.2025).

5. Прядка С. А. Кібербезпека як складова національної безпеки. С. 113–116. URL-адреса: https://doi.org/10.36059/978-966-397-491-0-33 (дата звернення: 22.10.2025).

6. Achten N. New U.N. Debate on Cybersecurity in the Context of International Security. URL: https://www.lawfaremedia.org/article/new-un-debate-cybersecurity-context-international-security (Last accessed: 08.10.25)

7. Arpentii S. Strategic principles of cybersecurity in the USA. Information and Law. 2025. No. 2(53). P. 176–182. URL: https://doi.org/10.37750/2616-6798.2025.2(53).334229 (Last accessed: 28.10.2025).

8. Bahromjonovich S. B. Problems of Iintellectual property rights protection in the digital space. International Journal of Law And Criminology. 2024. Vol. 4, no. 12. P. 98–108. URL: https://doi.org/10.37547/ijlc/volume04issue12-16 (Last accessed: 10.11.2025).

9. Barzilay O. Ways Blockchain Is Revolutionizing Cybersecurity . URL:https://www.forbes.com (Last accessed: 13.10.25).

10. Bracing for the Future of Information Security Threats. URL: https://www.infosecland.com (Last accessed: 15.10.25).

11. Bordoff S., Chen Q., Yan Z. Cyber Attacks, Contributing Factors, and Tackling Strategies. National Security. 2019. P. 60–77. URL: https://doi.org/10.4018/978-1-5225-7912-0.ch004 (Last accessed: 10.11.2025).

12. Buts C. Competition Policy's Travels through Cyberspace:. European Competition and Regulatory Law Review. 2017. Vol. 1, no. 1. P. 26–35. URL: https://doi.org/10.21552/core/2017/1/6 (Last accessed: 10.11.2025).

13. Competition and Restraint in Cyberspace: The Role of International Norms in Promoting U.S. Cybersecurity 2022. URL: https://www.rand.org/pubs/research_reports/RRA1180-1.html (Last accessed: 28.09.25)

14. Crootof R. The Law of Cyber-Attack. P. 853-877 URL: https://scholarship.richmond.edu/cgi/viewcontent.cgi?article=2608&context=law-faculty-publications (Last accessed: 18.10.25)

15. Cybersecurity and Infrastructure Security Agency (CISA). URL: https://www.cisa.gov (Last accessed: 12.10.25).

16. Cyber Security. Cyberspace & Sovereignty. 2022. P. 77–99. URL: https://doi.org/10.1142/9789811227790_0003 (date of access: 19.10.2025).

17. Cyber capabilities and national power of US. URL: https://www.iiss.org/globalassets/media-library---content--migration/files/research-papers/cyber-power-report/cyber-capabilities-and-national-power---united-states.pdf (Last accessed: 18.10.25)

18. Chavez P. Toward Digital Solidarity. URL: https://www.lawfaremedia.org/article/toward-digital-solidarity (date of access: 15.10.25).

19. Chinese Academy of Cyberspace Studi. Steady Improvement of Cybersecurity Safeguarding Capacity. China Internet Development Report 2018. Singapore, 2020. P. 89–101. URL: https://doi.org/10.1007/978-981-15-4043-1_6 (Last accessed: 09.11.2025).

20. Deibert R. Towards a Cyber Security Strategy for Global Civil society? URL: https://www.giswatch.org/en/freedom-expression/towards-cyber-security-strategy-global-civil-society (Last accessed: 05.10.25).

21. Durbin S. Bracing for the Future of Information Security Threats. URL: http://www.infosecisland.com/blogview/24905-Bracing-for-the-Future-of-Information-Security-Threats.html. (Last accessed: 16.10.25).

22. Eichensehr K., International Cyber Governance: Engagement Without Agreement? URL:https://www.justsecurity.org/19599/international-cyber-governance-engagement-agreement/ (Last accessed: 10.10.25)

23. Emary I., Brzozowska A. Shaping the Future of ICT: Trends in Information Technology, Communications Engineering, and Management. URL: https://doi.org/10.1201/9781315155241 (Last accessed: 14.10.25).

24. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu (Last accessed: 16.10.25).

25. European Union Agency for Network and Information Security (ENISA). Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches. URL: https://www.enisa.europa.eu (Last accessed: 12.10.25).

26. Farwell J., Rohozinski R. The New Reality of Cyber War. URL: https://indianstrategicknowledgeonline.com/web/New%20Reality%20of%20Cyber%20War.pdf (Last accessed: 02.11.25)

27. Fago, H.P. The implications of transnational cyber threats in international humanitarian law: analyzing the distinction between cybercrime, cyber-attack, and cyber warfare in the 21st century. 2017. P.1-34. URL: https://reference-global.com/2/v2/download/pdf/10.1515/bjlp-2017-0001 (Last accessed: 10.10.25)

28. Fidler David P. Final Acts of the World Conference on International Telecommunications. 2024. Vol. 52, No. 3. P. 843–860. URL: https://doi.org/10.5305/intelegamate.52.3.0843 (Last accessed: 15.10.25)

29. Fischer, E. A. Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions. URL: https://fas.org/sgp/crs/natsec/R42114.pdf (Last accessed: 08.10.25).

30. Fischerkeller, Michael P., Richard J. Harknett. Persistent Engagement, Agreed Competition, Cyberspace Interaction Dynamics, and Escalation. URL: https://www.ida.org/-/media/feature/publications/p/pe/persistent-engagement-agreed-competition-cyberspace-interaction-dynamics-and-escalation/d-9076.ashx (Last accessed: 11.10.25)

31. Forca B. Comparative analysis of national security strategies. 2023. URL: https://doi.org/10.70995/zjsw1372 (Last accessed: 10.11.2025).

32. Ford C. Cyberspace Security Diplomacy: Deterring Aggression in Turing's Monument. URL: https://2017-2021.state.gov/cyberspace-security-diplomacy-deterring-aggression-in-turings-monument/index.html (Last accessed: 15.10.25)

33. Gonzalez M.D. International Perspectives of Cyber Warfare. URL: https://doi.org/10.4018/IJCWT.2015100103 (Last accessed: 12.10.25)

34. Gourley, S. K. Cyber Sovereignty. Conflict and Cooperation in Cyberspace. 2016. P. 277–290. URL: https://doi.org/10.1201/b15253-16 (Last accessed: 19.11.2025).

35. Hathaway M.E. Preliminary Considerations: On National Cyber Security. P. 1-34. URL: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/hathaway-klimburg-nato-manual-ch-1.pdf (Last accessed: 08.10.25).

36. Havrilova L. H., Topolnik Y. V. Digital culture, digital literacy, digital competence as modern educational phenomena. Information technologies and learning tools. 2017. T. 61, № 5. P. 1-7. (Last accessed: 05.04.2024)

37. Hojda M. H. Information security economics: cyber security threats. Proceedings of the International Conference on Business Excellence. 2022. Vol. 16, no. 1. P. 584–592. URL: https://doi.org/10.2478/picbe-2022-0056 (Last accessed: 18.10.2025).

38. Hogeveen B. The UN norms of responsible state behaviour in cyberspace. URL: https://documents.unoda.org/wp-content/uploads/2022/03/The-UN-norms-of-responsible-state-behaviour-in-cyberspace.pdf (Last accessed: 20.11.25)

39. Holley P. Bill Gates on dangers of artificial intelligence. URL: https://www.washingtonpost.com/news/the-switch/wp/2015/01/28/bill-gates-on-

dangers-of-artificial-intelligence-dont-understand-why-some-people-are-not-concerned./?chead=true& (Last accessed: 08.10.25).

40. Iskuja I. Cybersecurity threats. SSRN electronic journal. 2024. URL: https://doi.org/10.2139/ssrn.4723335 (Last accessed: 05.09.2025)

41. International Cybersecurity Information Sharing Agreements. URL: https://cissm.umd.edu/sites/default/files/2019-07/Cyber%20information%20sharing %20agreement%20report%20-%20102017%20-%20FINAL.pdf (Last accessed: 05.10.25)

42. International Telecommunication Union (ITU). 2022. Global Cybersecurity Index 2022. URL: https://www.itu.int (Last accessed: 05.10.25)

43. Implications for State Sovereignty. Cyber Sovereignty. 2024. P. 154–172. URL: https://doi.org/10.1515/9781503639386-009 (Last accessed: 10.11.2025).

44. Juzenaite R., Dimov D., Crowdsourcing Cybersecurity: How to Raise Security Awareness Through Crowdsourcing. URL: https://www.infosecinstitute.com/crowdsourcing-cybersecurity-how-to-raise-security-awareness-through-crowdsourcing./ (Last accessed: 12.10.25).

45. Juzenaite R., Dimov D. Cyber Attack Protection via Crowdsourcing. URL: https://www.infosecinstitute.com/cyber-attack-protection-via-crowdsourcing./ (Last accessed: 12.10.25)

46. Kerry J. An Open and Secure Internet: We Must Have Both. URL:https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm (Last accessed: 20.10.25)

47. Klimburg A., Almeida, Virgilio A.F. Cyber Peace and Cyber Stability: Taking the Norm Road to Stability. URL: https://ieeexplore.ieee.org/document/8874985 (Last accessed: 12.10.25)

48. Korzak E. International Law and the UN GGE Report on Information Security. URL: https://www.justsecurity.org/28062/international-law-gge-report-information-security/ (Last accessed: 05.10.25)

49. Korzak E. UN GGE on Cybersecurity: The End of an Era? URL: https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/ (Last accessed:11.11.2025)

50. Lonergan E., Lonergan S. To Defend Forward, the U.S. Must Strengthen the Cyber Mission Force. URL: https://www.lawfaremedia.org/article/defend-forward-us-must-strengthen-cyber-mission-force (Last accessed: 14.10.25)

51. Lunden I. Microsoft to Buy Israeli Security Firm Hexadite, Sources Say for $100M . URL: https://techcrunch.com (Last accessed: 08.10.25).

52. Lunden I. More Funding for AI Cybersecurity: Darktrace Raises $75M at an $825M Valuation. URL:https://techcrunch.com (Last accessed: 12.10.25).

53. Marks J. U.S. Makes New Push for Global Rules in Cyberspace. URL: https://www.politico.com/story/2015/05/us-makes-new-push-for-global-rules-in-cyberspace-117632 (Last accessed: 16.11.25)

54. McKay A., Nicholas P., Neutze J., Sullivan K. International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World. URL: file:///C:/Users/nasty/Downloads/International_Cybersecurity_%20Norms.pdf (Last accessed: 01.11.2025).

55. McKune Sarah. An Analysis of the International Code of Conduct for Information Security. URL: https://citizenlab.ca/2015/09/international-code-of-conduct/ (Last accessed: 15.10.25).

56. Microsoft Security Intelligence. Cyber Threat Trends. 2023. URL: https://www.microsoft.com (Last accessed: 10.11.2025).

57. Choucri N., Madnick S., Ferwerda J. Institutions for cyber security: international responses and global imperatives. P. 96-121. URL: https://dspace.mit.edu/handle/1721.1/109401 (Last accessed: 11.11.25).

58. National Institute of Standards and Technology (NIST). Cybersecurity Framework. URL: https://www.nist.gov (Last accessed: 15.10.25).

59. Nakashima E. U.S. Cyberwarfare Force To Grow Significantly, Defense Secretary Says. URL: http://www.washingtonpost.com/world/national-security/us-cyberwarfare-force-to-grow-significantly-defense-secretary-

says/2014/03/28/0a1fa074-b680-11e3-b84e-897d3d12b816_story.html (Last accessed: 12.10.25).

60. Osula A, Rõigas H. International Cyber Norms. URL: https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf?utm_source=chatgpt.com (Last accessed: 20.10.25)

61. Pietras E. Information security – its essence and threats. Scientific Journal of the Military University of Land Forces. 2019. Vol. 191, no. 1. P. 26–35. URL: https://doi.org/10.5604/01.3001.0013.2396 (Last accessed: 01.11.2025).

62. Report on the Cybersecurity Posture of the United States. 2024. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf (Last accessed: 13.10.25)

63. Shen Y. Cyber Sovereignty and the Governance of Global Cyberspace. Chinese Political Science Review. 2016. P. 81–93. URL: https://doi.org/10.1007/s41111-016-0002-6 (Last accessed: 19.10.2025).

64. Sussex M., Clarke M., Medcalf R. National security: between theory and practice. Australian Journal of International Affairs. 2017. Vol. 71, no. 5. P. 474–478. URL: https://doi.org/10.1080/10357718.2017.1347139 (Last accessed: 10.11.2025).

65. Stamp M. Introduction to Machine Learning with Applications in Information Security. URL: https://de.scribd.com/document/701117520/Mark-Stamp-Introduction-to-Machine-Learning-With-Applications-in-Information-Security-previewpdf (Last accessed: 15.10.25)

66. Rosenberg S. Firewalls Don't Stop Hackers. AI Might. URL: https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might (Last accessed: 11.10.2025)

67. Ruubel M. U.S. Department of Energy Contracts Guardtime, Siemens and Industry Partners for Blockchain Cybersecurity Solution. URL: https://guardtime.com (Last accessed: 10.10.25).

68. SWIFT Launches the “SWIFT Information Sharing and Analysis Centre”. URL: https://www.swift.com (Last accessed: 10.10.25).

69. The United States and Interdependence Sovereignty. Cyber Sovereignty. 2024. P. 130–153. URL: https://doi.org/10.1515/9781503639386-008 (Last accessed: 11.11.2025).

70. United Nations. Secretary General. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. July 2015. URL: https://digitallibrary.un.org/record/799853?ln=en&v=pdf (Last accessed: 10.10.25).

71. Preserving America's Cyber Sovereignty. URL: https://americanmind.org/memo/preserving-americas-cyber-sovereignty/ (Last accessed: 16.10.25).

72. Singer P. W., Friedman A. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford: Oxford University Press, 2014. 320 c.

73. Tershukov D. Analysis of Modern Information Security Threats. NBI Technologies. 2019. No.3. P. 6–12. URL: https://doi.org/10.15688/nbit.jvolsu.2018.3.1 (Last accessed: 19.10.2025).

74. Tikk E., Kaska K., Vihul L. International Cyber Incidents: Legal Considerations. NATO Cooperative Cyber Defence Centre of Excellence. P. 15-45. URL: https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf (Last accessed: 05.11.25)

75. Toward Digital Solidarity. URL: https://www.lawfaremedia.org/article/toward-digital-solidarity (Last accessed: 12.10.24).

76. The White House National Cybersecurity Strategy. URL: https://www.whitehouse.gov (Last accessed: 13.10.25).

77. The United Nations, Cyberspace and International Peace and Security (UNIDIR). URL: https://unidir.org/files/publication/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf (Last accessed: 16.10.25)

78. United Nations Group of Governmental Experts (GGE). Advancing Responsible State Behavior in Cyberspace. URL: https://www.un.org (Last accessed: 11.10.24).

79. Restrictions on access to public information in the national security interests, three-part test. URL: https://www.magnanimitas.cz/ADALTA/120231/papers/A_30.pdf (Last accessed: 16.10.25).

80. Unpacking the GGE's framework on responsible state behaviour:Cyber norms. URL: https://www.apc.org/sites/default/files/UnpackingGGGCyberNorms.pdf (Last accessed: 16.10.25).

81. World Economic Forum. Global Cybersecurity Outlook 2023. URL: https://www.weforum.org (Last accessed: 10.10.25).

82. What is the future of cyber security? URL: https://www.telegraph.co.uk/business/ (Last accessed: 10.11.2025).

83. What Will Cybersecurity Look Like 10 Years From Now? URL: https://www.forbes.com/sites/quora/2017/09/14/what-will-cybersecurity-look-like-10-years-from-now./ (Last accessed: 11.10.25).

84. Ways Blockchain Is Revolutionizing Cybersecurity. URL: https://www.forbes.com (Last accessed: 10.10.25).

85. Yalman Y., Yesilyurt M. Information Security Threats and Information Assurance. P. 247–252. URL: https://doi.org/10.18421/tem23-07 (Last accessed: 15.10.2025).

АНОТАЦІЯ

Зеленська А.О. Кіберсувернітет США як складова національної та глобальної інформаційної безпеки (магістерська робота). Харків: ХНУ імені В. Н. Каразіна, 2025. 83 с. (рукопис).

Мета кваліфікаційної роботи полягає у визначенні особливостей формування кіберсуверенітету США як складової національної та глобальної інформаційної безпеки.

Об'єктом дослідження є система національної та глобальної інформаційної безпеки.

Предметом дослідження є кіберсуверенітет США як складова національної та глобальної інформаційної безпеки.

У першому розділі здійснюється теоретико-методологічне обґрунтування феномену інформаційної безпеки. Досліджується зміст і структура поняття «інформаційна безпека» та його місце в системі національної безпеки.

Другий розділ присвячено дослідженню кіберсуверенітету як структурного елементу національної інформаційної безпеки США. Розкривається еволюція підходів США до формування кіберсуверенітету, а саме від моделі відкритого Інтернету до сучасних концепцій цифрового захисту.

У третьому розділі досліджується вплив США на формування глобальної архітектури інформаційної безпеки. Аналізується роль Сполучених Штатів у виробленні міжнародних норм, стандартів і принципів регулювання інформаційного простору. Розкриваються механізми взаємодії США з міжнародними організаціями у сфері кіберполітики та інформаційної безпеки.

Ключові слова: кіберполітика, кіберсуверенітет, національна безпека, США, цифровий захист, інформаційна безпека.

ANNOTATION

Zelenska A.O. Cyber Sovereignty of the United States as a Component of National and Global Information Security (Master's Thesis). Kharkiv: V. N. Karazin Kharkiv National University, 2025. 83 p. (manuscript).

The purpose of the qualification thesis is to determine the specific features of the formation of the cyber sovereignty of the United States as a component of national and global information security.

The object of the study is the system of national and global information security.

The subject of the study is the cyber sovereignty of the United States as a component of national and global information security.

The first chapter provides a theoretical and methodological substantiation of the phenomenon of information security. It examines the content and structure of the concept of "information security" and its place within the system of national security.

The second chapter focuses on the study of cyber sovereignty as a structural element of the United States' national information security. It reveals the evolution of U.S. approaches to the formation of cyber sovereignty – from the model of an open Internet to modern concepts of digital protection.

The third chapter explores the influence of the United States on the formation of the global architecture of information security. It analyzes the role of the United States in developing international norms, standards, and principles for regulating the information space. The mechanisms of the United States' interaction with international organizations in the field of cyber policy and information security are examined.

Keywords: cyber policy, cyber sovereignty, national security, United States, digital protection, information security.

ВІДГУК

керівника кваліфікаційної роботи магістра
2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії» освітньо-професійної програми
«Міжнародна інформаційна безпека»
ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Зеленської Анастасії Олегівни
на тему: «Кіберсуверенітет США як складова національної та глобальної інформаційної безпеки»

Тема роботи «Кіберсуверенітет США як складова національної та глобальної інформаційної безпеки» є досить актуальною, оскільки стрімка цифровізація всіх сфер суспільного життя, зростання масштабів кібератак та посилення конкуренції між державами у кіберпросторі перетворюють питання контролю, захисту та управління цифровими ресурсами на ключовий фактор національної безпеки. США, як одна з провідних кібердержав, формують глобальні стандарти реагування на кіберзагрози, а їхня політика значною мірою визначає архітектуру міжнародної кібербезпеки. У цих умовах дослідження кіберсуверенітету США дозволяє зрозуміти механізми забезпечення інформаційного суверенітету сучасних держав, оцінити ризики та перспективи глобального кіберуправління, а також визначити, яким чином США впливають на міжнародні норми та правила у сфері кібербезпеки у відповідь на новітні геополітичні виклики.

За структурою робота відповідає вимогам послідовного та логічного розкриття змісту і складається зі вступу, трьох розділів, висновків, переліку використаних джерел. Побудова кваліфікаційної роботи дозволяє у повному обсязі з позиції системності та у логічній послідовності викласти матеріал і надати вичерпну характеристику проведеному дослідженню у теоретичній, аналітичній та результативній частині.

Перший розділ роботи «Теоретичні засади дослідження національної та глобальної інформаційної безпеки» присвячено визначенню сутності

національної та глобальної інформаційної безпеки, особливостям нормативно-правової бази забезпечення національної інформаційної безпеки США.

У другому розділі «Кіберсувернітет США в системі національної інформаційної безпеки» було розкрито концептуальний зміст кіберсуверенітету та його місце у загальній архітектурі національної інформаційної безпеки, виокремлено особливості становлення та інституційного забезпечення кіберсуверенітету США.

Третій розділ роботи «Кіберсувернітет США як чинник формування глобальної інформаційної безпеки» присвячено оцінці ролі США у формуванні міжнародних норм і стандартів у сфері інформаційної безпеки, визначенню їхньої взаємодії з ключовими міжнародними організаціями, виявленню основних викликів та перспективних напрямів розвитку кіберсуверенітету США в сучасній системі глобальної інформаційної безпеки.

Висновки, отримані авторкою у процесі виконання кваліфікаційної роботи магістра, є повними, обґрунтованими та повністю розкривають поставлену мету та визначені завдання. Список використаних джерел досить повний і містить вітчизняні та зарубіжні джерела за обраною тематикою.

Робота є комплексним самостійним дослідженням, добре структурована.

У цілому кваліфікаційна робота магістра на тему: «Кіберсуверенітет США як складова національної та глобальної інформаційної безпеки» заслуговує на високу оцінку, а її авторка, Зеленська Анастасія Олегівна, гідна присвоєння кваліфікації магістра міжнародних відносин, суспільних комунікацій та регіональних студій.

Керівник кваліфікаційної роботи,
кандидат економічних наук,
доцент, доцент кафедри
міжнародних відносин Лариса ЧЕРНИШОВА

РЕЦЕНЗІЯ

на кваліфікаційну роботу магістра
2-го курсу групи УМІБ-61 денної форми навчання
спеціальності 291 «Міжнародні відносини, суспільні комунікації та регіональні студії» освітньо-професійної програми
«Міжнародна інформаційна безпека»
ННІ «Каразінський інститут міжнародних відносин та туристичного бізнесу»
Харківського національного університету імені В.Н. Каразіна
Зеленської Анастасії Олегівни
на тему: «Кіберсуверенітет США як складова національної та глобальної інформаційної безпеки»

Актуальність дослідження кіберсуверенітету США як складової національної та глобальної інформаційної безпеки зумовлена стрімким зростанням кіберзагроз, що перетворюють цифровий простір на ключовий вимір міжнародної безпеки. Сполучені Штати, як одна з провідних світових кібердержав, формують стандарти, політики й технологічні підходи, які впливають не лише на власний національний захист, але й на глобальну архітектуру кіберуправління. Зростання масштабів кібератак, інформаційних операцій, втручань у виборчі процеси та загрози критичній інфраструктурі підсилюють потребу у вивченні того, як США визначають і реалізують свій кіберсуверенітет. Дослідження цієї теми дає можливість оцінити ефективність американських стратегій, їхній вплив на міжнародні норми та потенційні конфлікти між принципами відкритого інтернету й прагненням до зміцнення національного контролю над цифровим простором.

У кваліфікаційній роботі магістра визначено мету та завдання, вирішенню яких присвячено три розділи кваліфікаційної роботи. Перший розділ роботи «Теоретичні засади дослідження національної та глобальної інформаційної безпеки» присвячено визначенню сутності національної та глобальної інформаційної безпеки, особливостям нормативно-правової бази забезпечення національної інформаційної безпеки США.

У другому розділі «Кіберсувернітет США в системі національної інформаційної безпеки» було розкрито концептуальний зміст кіберсуверенітету та його місце у загальній архітектурі національної інформаційної безпеки, виокремлено особливості становлення та інституційного забезпечення кіберсуверенітету США.

Третій розділ роботи «Кіберсувернітет США як чинник формування глобальної інформаційної безпеки» присвячено оцінці ролі США у формуванні міжнародних норм і стандартів у сфері інформаційної безпеки,

визначенню їхньої взаємодії з ключовими міжнародними організаціями, виявленню основних викликів та перспективних напрямів розвитку кіберсуверенітету США в сучасній системі глобальної інформаційної безпеки.

Висновки, отримані здобувачкою вищої освіти у процесі виконання кваліфікаційної роботи магістра, є повними, обґрунтованими, повністю розкривають поставлену мету та визначені завдання. Список використаних джерел є повним і містить вітчизняні та зарубіжні джерела за обраною тематикою.

Робота є комплексним самостійним дослідженням, добре структурована. Під час виконання кваліфікаційної роботи авторка показала високий рівень підготовки та знань з обраної теми, вміння самостійно аналізувати та систематизувати матеріал, робити висновки та узагальнення.

Питання, визначені в роботі, розкриті, але вони мають окремі недоліки. Так, у пункті 3.3 «Виклики та перспективи розвитку кіберсуверенітету США в системі глобальної інформаційної безпеки» сучасні загрози кіберсуверенітету США були проаналізовані недостатньо глибоко та без належної прив'язки до конкретних стратегічних рішень, ухвалених американськими урядовими інституціями, проте це не зменшує цінності самої роботи.

У цілому кваліфікаційна робота магістра на тему: «Кіберсуверенітет США як складова національної та глобальної інформаційної безпеки» заслуговує на оцінку «відмінно», а її авторка, Зеленська Анастасія Олегівна, гідна присвоєння кваліфікації магістра міжнародних відносин, суспільних комунікацій та регіональних студій.

Рецензент:

завідувач кафедри політології,
соціології і культурології
Харківського національного
педагогічного університету
імені Г. С. Сковороди,
кандидат політичних наук, доцент Олександр БЕЗРУК

Підпис Безрука О.В.
засвідчується зав. канцелярією
01.12.2025