Кам’янець-Подільський національний університет імені Івана Огієнка
Історичний факультет
Кафедра політології та філософії

Кваліфікаційна робота
бакалавра
з теми: «Політичні аспекти кібербезпеки: ризики та виклики для України»

Виконала:
студентка 4 курсу, групи Р1-В22
першого (бакалаврського) рівня вищої освіти
спеціальності 052 Політологія
денної форми здобуття вищої освіти
Жук Валерія

Керівник:
Віннічук О. В., кандидат політичних наук,
доцент, доцент кафедри політології та філософії

Рецензент:

_____

Кам’янець-Подільський
2026

ЗМІСТ

ВСТУП 3

РОЗДІЛ 1 ТЕОРЕТИКО-ПОЛІТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ ЯК СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ 6

1.1 Сутність кібербезпеки та її місце в системі національної безпеки держави6

1.2 Політичні чинники формування державної політики у сфері кібербезпеки 13

1.3 Нормативно-правові засади забезпечення кібербезпеки в Україні..... 19

РОЗДІЛ 2 ПОЛІТИЧНІ РИЗИКИ ТА ЗАГРОЗИ КІБЕРБЕЗПЕЦІ УКРАЇНИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ 30

2.1 Державна стратегія кібербезпеки України та її політичні пріоритети 30

2.2. Зовнішні та внутрішні політичні загрози як інструмент гібридної війни .. 36

2.3 Міжнародне політичне співробітництво України у сфері кібербезпеки та обміну даними 42

ВИСНОВКИ 47

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ 49

ВСТУП

Стрімка цифровізація суспільно-політичних, економічних і управлінських процесів у XXI столітті сприяла трансформації уявлень про безпеку держави та змінила характер загроз її суверенітету й стабільності. Кіберпростір перетворився на повноцінний вимір політичного протистояння, у якому реалізуються як внутрішньополітичні, так і зовнішньополітичні інтереси держав. День 24 лютого 2022 р. назавжди залишиться в історії чорним днем військового вторгнення Росії в Україну [8]. В умовах російсько-української війни питання кібербезпеки набуло особливої актуальності, оскільки є одним із ключових інструментів гібридної війни, спрямованої на підрив діяльності державних інституцій, критичної інфраструктури та формування громадської думки. Саме поєднання військових дій із системними кібератаками, інформаційними операціями та політичним тиском визначає сучасну логіку безпекових викликів для України.

Актуальність дослідження зумовлена тим, що кіберзагрози для України мають не лише технічний, а передусім політичний характер. Кібератаки проти органів державної влади, енергетичного сектору, фінансових установ і державних електронних сервісів у 2015–2025 роках продемонстрували здатність впливати на прийняття політичних рішень, дестабілізувати процеси державотворення та формувати міжнародний порядок денний. Масштабні інциденти, зокрема атаки на енергетичну інфраструктуру у 2015 році та 2017 році, засвідчили, що кібероперації можуть мати наслідки, співмірні з традиційними актами агресії. Повномасштабне вторгнення рф в Україну у 2022 році остаточно закріпило кіберпростір як невід'ємну складову воєнних дій і державної безпекової політики.

Політичний вимір кібербезпеки проявляється у формуванні стратегій, нормативно-правових актів, інституційної архітектури та міжнародної співпраці. Державна стратегія кібербезпеки України 2021 року стала відповіддю на накопичений досвід гібридної агресії та зафіксувала пріоритети захисту

критичної інфраструктури, міжвідомчої координації, інтеграції до європейських і євроатлантичних безпекових структур. У цьому контексті дослідження політичних аспектів кібербезпеки є необхідним для комплексного розуміння сучасних ризиків і викликів, що постають перед Україною.

Об'єктом дослідження є кібербезпека як складова національної безпеки держави.

Предметом дослідження є політичні аспекти формування та реалізації державної політики у сфері кібербезпеки України в умовах російсько-української війни.

Метою дипломної роботи є комплексний аналіз політичних ризиків і викликів у сфері кібербезпеки України, а також визначення ролі державної стратегії, гібридних загроз і міжнародного співробітництва у забезпеченні національної стійкості у кіберпросторі.

Для досягнення поставленої мети у роботі визначено **такі завдання:**

1) розкрити сутність кібербезпеки та визначити її місце в системі національної безпеки держави;

2) проаналізувати політичні чинники формування державної політики у сфері кібербезпеки;

3) охарактеризувати Державну стратегію кібербезпеки України та її політичні пріоритети в умовах війни;

4) дослідити зовнішні й внутрішні політичні загрози кібербезпеці України як інструменти гібридної війни;

5) проаналізувати роль міжнародного політичного співробітництва та обміну даними у зміцненні кіберстійкості держави.

Методологічну основу дослідження становить сукупність загальнонаукових і спеціальних методів пізнання. Використано методи аналізу та синтезу для осмислення теоретичних підходів до кібербезпеки й узагальнення політичних чинників її формування; системний метод для розгляду кібербезпеки як елементу національної безпеки; історичний метод для аналізу еволюції кіберзагроз і державної політики України у 2015–2025 роках; структурно-

функціональний метод для дослідження інституційної архітектури кібербезпеки; порівняльний метод для зіставлення національних і міжнародних підходів до кіберзахисту; формально-правовий метод для аналізу стратегічних і нормативно-правових документів.

Практичне значення одержаних результатів полягає в можливості використання висновків роботи у навчальному процесі з дисциплін, пов'язаних із національною безпекою, політичною безпекою та міжнародними відносинами, а також у подальших дослідженнях проблем кібербезпеки України. Матеріали роботи можуть бути корисними для аналітичної діяльності у сфері державної безпекової політики та для формування експертних оцінок щодо кіберризиків в умовах гібридної війни.

Апробація результатів дослідження. Результати дослідження були апробовані під час наукової конференції студентів і магістрантів за підсумками НДР у 2024-2025 навчальному році (м. Кам'янець-Подільський, 9-10 квітня 2026 р.)

Публікації. Подано до публікації тези на тему: "Гібридна війна як інструмент політичного впливу". Філософ-і-Я: наукові розвідки студентів Кам'янець-Подільського національного університету імені Івана Огієнка : наук. журнал / гол. ред. А.В. Найчук. Кам'янець-Подільський : Кам'янець-Подільський національний університет імені Івана Огієнка, 2026. Випуск 11.

Структура дипломної роботи зумовлена метою та завданнями дослідження і включає вступ, два розділи, висновки та список використаних джерел.

РОЗДІЛ 1 ТЕОРЕТИКО-ПОЛІТИЧНІ ОСНОВИ КІБЕРБЕЗПЕКИ ЯК СКЛАДОВОЇ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

1.1 Сутність кібербезпеки та її місце в системі національної безпеки держави

Сучасна епоха характеризується тотальною цифровізацією всіх суспільних процесів, що докорінно змінює архітектуру світового порядку та змушує переосмислювати класичні парадигми безпеки. Розуміння кібербезпеки в сучасному науковому дискурсі вже давно вийшло за межі суто технічного захисту інформації та базується на кількох фундаментальних підходах, що взаємодоповнюють один одного. Техніко-технологічний підхід фокусується на забезпеченні стійкості програмно-апаратних комплексів, впровадженні передових криптографічних методів захисту даних та постійній мінімізації технологічних вразливостей. Правові та організаційні основи забезпечення кібербезпеки України визначають повноваження та відповідальність суб'єктів забезпечення кібербезпеки, основні вимоги до управління кібербезпекою, порядок реагування на кіберінциденти та кібератаки, а також створення Національної системи кібербезпеки як сукупності суб'єктів забезпечення кібербезпеки, об'єднаних єдиною політикою та координацією їх діяльності [1].

Як слушно зазначає М.Т. Гаврильців, інформаційна безпека є складовою частиною загальної системи національної безпеки країни і становить сукупність органів державної влади, недержавних структур і громадян, які повинні узгоджено здійснювати діяльність із забезпечення інформаційної безпеки на основі єдиних правових норм, ефективно протистояти інформаційним загрозам за сучасних умов [5, с. 203].

Як зазначають В.С. Виздрик та О.М. Мельник, інформаційна безпека не обмежується захистом від несанкціонованого доступу до інформації, а є принципово ширшим поняттям, адже суб'єкт інформаційних відносин може постраждати не тільки в результаті несанкціонованого доступу, але й внаслідок системного збою, що призвів до переривання роботи [4, с. 197]. Інформаційна безпека — це багатогранна сфера діяльності, в якій тільки системний, комплексний підхід

може привести до успіху [4, с. 196]. Обсяг проблем, пов'язаних з використанням інформаційних систем, можна розділити на наступні категорії: забезпечення доступності, цілісності та конфіденційності інформаційних ресурсів і допоміжної інфраструктури [4, с. 196]. У цьому контексті особливого значення набуває захист критичної інформаційної інфраструктури, оскільки будь-яке деструктивне втручання у роботу енергетичних мереж, транспортних вузлів або систем державного зв'язку може призвести до катастрофічних наслідків національного масштабу.

Для України, яка протягом тривалого часу перебуває в стані активної відсічі зовнішній збройній агресії, питання кіберзахисту перетворилося з вузькопрофільного технічного завдання на критичний стратегічний пріоритет, що нерозривно інтегрований у загальну архітектуру національної безпеки держави [8; 47]. Як зазначено на офіційному сайті НАТО, у липні 2016 року союзники підтвердили оборонний мандат Альянсу та визнали кіберпростір доменом операцій [27]. Це визнання кіберпростору окремим доменом оборони, аналогічним суходолу, морю чи повітряному простору, вимагає від оборонного сектору формування якісно нової архітектури стримування та протидії. Після початку війни Росії проти України серед перших прикладів кібервійни були: атака на системи зв’язку газети «Kyiv Post» та супутникову мережу «KA-SAT» за годину до вторгнення (24 лютого), атака IssacWiper на урядові вебсайти (25 лютого), кібератака на пункт прикордонного контролю з метою перешкоджання виїзду біженців до Румунії (25 лютого) та атаки на цифрову інфраструктуру України, що призвело до блокування доступу до фінансових послуг та енергетичних ресурсів (28 лютого) [16, с. 2].

В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення різновекторних національних інформаційних інтересів, поширення інформаційної експансії та агресії, захист національного інформаційного простору та гарантування інформаційної безпеки стають пріоритетними стратегічними завданнями сучасних держав у системі глобальних інформаційних відносин [10, с. 28]. Аналізуючи кібербезпеку як невід'ємну складову національної безпеки, необхідно підкреслити її інтегративну природу. Вона не існує ізольовано, а пронизує політичні, правові, військові та економічні інструменти державної

політики. Політичний аспект кібербезпеки полягає у здатності влади формувати безпековий порядок денний та забезпечувати довіру громадян до цифрових інститутів. Військовий вимір передбачає готовність збройних сил до ведення операцій у кіберпросторі, захист систем управління військами та протидію цифровому шпигунству [26]. Економічний складник фокусується на захисті інтелектуальної власності, стабільності банківської системи та підтримці інноваційного потенціалу країни. Кібербезпека стає фундаментом національної стійкості, забезпечуючи безперервність функціонування державних інститутів у глобалізованому світі. Головною загрозою інформаційній безпеці нашої держави залишається загроза впливу ворога на інформаційну інфраструктуру, інформаційні ресурси, суспільство, свідомість і підсвідомість особистості з метою нав’язати власну систему цінностей, поглядів, інтересів і рішень у життєво важливих сферах суспільної й державної діяльності [14].

Еволюція ролі кібербезпеки протягом останнього десятиліття демонструє перехід від захисту окремих вузлів до формування глобальних контурів цифрової оборони. Середина 2010-х років стала точкою перелому, коли кібератаки почали використовуватись не лише кримінальними угрупованнями для фінансової наживи, а й державними суб'єктами як елемент геополітичного тиску [3]. Як зазначається у звіті американської агенції CISA, "23 грудня 2015 року українські енергетичні компанії зазнали позапланових відключень електроенергії, які вплинули на велику кількість споживачів в Україні. Кібератака була синхронізованою та скоординованою, ймовірно, після масштабної розвідки мереж жертв. Протягом кібератаки здійснювалося зловмисне дистанційне керування вимикачами кількома зовнішніми особами» [28]. Цей інцидент продемонстрував, що кіберзброя здатна завдавати цілком реальної, фізичної шкоди національній інфраструктурі. Подальша ескалація в кіберпросторі призвела до поширення у 2017 році вірусу NotPetya, який, хоч і був спрямований проти української фінансової системи, спричинив глобальний колапс великих міжнародних корпорацій [35; 43]. Як повідомляє CISA, "всі три компанії зазначили, що зловмисники наприкінці кібератаки виконали шкідливе програмне забезпечення KillDisk, яке видаляє вибрані файли на цільових системах і пошкоджує головний завантажувальний запис, роблячи системи

непрацездатними. Крім того, зловмисники зробили непрацездатними послідовно- Ethernet-пристрої на підстанціях, пошкодивши їхнє мікропрограмне забезпечення" [28].

Національна система кібербезпеки будь-якої сучасної держави базується на розбудові специфічних інституційних рамок. В Україні цей процес отримав потужний імпульс у 2016 році з прийняттям першої Стратегії кібербезпеки, яка заклала підвалини міжвідомчої координації [3]. Подальше вдосконалення інституційної архітектури дозволило чітко розмежувати повноваження між суб'єктами забезпечення кібербезпеки [1]. Спеціалізовані підрозділи, як-от CERT-UA (Урядова команда реагування на комп'ютерні надзвичайні події), відіграють роль оперативного штабу, який не лише реагує на поточні загрози, а й здійснює постійний аналіз трендів у кіберпросторі [7; 17].

Особливе місце в ієрархії безпекових пріоритетів займає людський капітал, що виступає інтелектуальним щитом нації. Підготовка висококваліфікованих кадрів, здатних до стратегічного аналізу та прийняття рішень в умовах високої невизначеності гібридної війни, є питанням виживання держави [20, с. 156; 21]. Це завдання охоплює не лише вузькоспеціалізовану підготовку кіберінженерів, а й системне підвищення рівня кібергігієни серед державних службовців та широких верств населення [11]. Транскордонна природа сучасного інтернету робить будь-який ізольований захист апріорі неефективним, що висуває на перший план міжнародну співпрацю як невід'ємний елемент національної стратегії [45; 47].

Стратегічний вимір кібербезпеки нерозривно пов'язаний із концепцією кіберстримування. Сучасні держави прагнуть не лише захищатись, а й створювати такі умови, за яких потенційний агресор усвідомлюватиме неприпустимо високу ціну атаки. Як зазначається в офіційних документах НАТО, кіберпростір є контестованим у будь-який час, а зловмисні кіберінциденти відбуваються щодня – від низькорівневих до технологічно складних атак. У цьому контексті Альянс розвиває спроможності виявляти, запобігати та реагувати на зловмисну кібердіяльність, а кібероборона є частиною базового завдання НАТО – стримування та оборони [27]. Це досягається через поєднання надійного захисту (стримування шляхом заперечення вигоди) та

готовності до асиметричної відповіді (стримування шляхом покарання). У цьому контексті кіберзахист інтегрується з традиційними формами ведення війни, інформаційними операціями та дипломатичними інструментами [33].

Концептуальною основою розбудови національної системи кібербезпеки в Україні, як наголошує В.І. Ящук, є три ключові принципи: стримування, кіберстійкість та сприяння взаємодії. Стримування передбачає посилення спроможностей для запобігання збройній агресії у кіберпросторі, нейтралізацію розвідувально-підривної діяльності та мінімізацію загроз кіберзлочинності й кібертероризму. Кіберстійкість означає здатність швидко адаптуватися до внутрішніх і зовнішніх загроз, підтримуючи стабільне функціонування національної інформаційної інфраструктури, зокрема об'єктів критичної інфраструктури. Сприяння взаємодії забезпечує розвиток комунікації, координації та партнерства між усіма суб'єктами забезпечення кібербезпеки на національному рівні [23, с. 6-7].

Важливо враховувати, що значна частина цифрового простору та критичних активів перебуває у власності приватних корпорацій. Тому державна політика має включати гнучкі механізми стимулювання бізнесу до інвестицій у безпеку [29; 42]. Інтеграція приватного сектору до системи національної безпеки відбувається через спільні навчання та створення платформ для добровільного обміну інформацією про інциденти [7; 17].

Важливим аспектом сучасного розуміння кібербезпеки є визнання її динамічного характеру. Як засвідчують дані Державної служби спеціального зв'язку та захисту інформації України, кількість зареєстрованих кіберінцидентів зросла з 1350 у 2021 році до 4315 у 2024 році, що демонструє чітку ескалацію використання кібервійни з боку Російської Федерації. Особливо показовим є зменшення кількості критичних інцидентів з 1048 у 2022 році до 59 у 2024 році, що свідчить про підвищення спроможностей України зменшувати деструктивний вплив кібератак» [47, с. 6]. На відміну від традиційних сфер безпеки, де загрози можуть бути відносно стабільними та передбачуваними, кіберпростір характеризується стрімкою зміною тактик, технік і процедур (TTP) зловмисників. Це вимагає від державних інституцій не лише реактивного реагування на вже відомі інциденти, а й проактивного прогнозування майбутніх

загроз на основі аналізу розвідувальних даних та поведінкових патернів [16]. У цьому контексті особливого значення набувають підрозділи кіберрозвідки, здатні виявляти підготовку до атак на ранніх стадіях, а також системи раннього попередження, інтегровані в національну архітектуру кібербезпеки [27; 42].

Сучасна парадигма кібербезпеки також передбачає перехід від моделі «захисту периметра» до концепції «нульової довіри» (Zero Trust). Ця концепція базується на принципі, що жоден користувач, пристрій або мережевий трафік не може вважатися безумовно надійним, навіть якщо вони перебувають всередині корпоративної чи державної мережі. Кожен запит на доступ до ресурсів має проходити автентифікацію, авторизацію та шифрування, а доступ надається за принципом «найменших привілеїв» [42; 47]. Впровадження цієї моделі в державних інформаційних системах України, особливо в умовах воєнного стану, дозволило значно знизити ризики компрометації критичних даних через скомпрометовані облікові записи або внутрішні загрози [7; 17].

Не менш значущим є розуміння кібербезпеки як сфери, що потребує постійного балансування між заходами захисту та забезпеченням фундаментальних прав і свобод громадян. Масовий збір даних, тотальний моніторинг комунікацій та розширення повноважень спецслужб у кіберпросторі, хоч і є ефективними інструментами протидії загрозам, водночас створюють ризики для приватності та громадянських свобод [10, с. 28]. В Україні, яка перебуває в стані збройної агресії, цей баланс тимчасово зміщений у бік безпекових заходів, що передбачено законодавством про правовий режим воєнного стану. Однак навіть у цих умовах зберігається необхідність демократичного контролю за діями уповноважених органів, зокрема через парламентський нагляд та судовий контроль за застосуванням найбільш чутливих інструментів [1; 47].

Особливої уваги заслуговує питання кібербезпеки в контексті захисту критичної інфраструктури в умовах гібридної війни. У звіті Держспецзв'язку наголошується, що енергетичний сектор є базовим рівнем ІТ-екосистеми: "Без електрики зупиняється робота установ та організацій, не працює логістика, немає координації, настає параліч усіх інших елементів піраміди. Відсутність електроенергії призводить до втрати зв'язку, тепла, паніки та порушує

життєзабезпечення ключових систем". Телекомунікації визначено як ключове середовище передачі інформації, а ІТ-системи — як основа для роботи банків, фінансів, логістики та державних реєстрів» [47, с. 7]. Енергетичний сектор, система водопостачання, транспортні вузли та зв'язок є пріоритетними цілями для кібератак, оскільки їх виведення з ладу може мати катастрофічні наслідки для цивільного населення та обороноздатності держави [8, с. 22]. Досвід атак на українську енергосистему в 2015 та 2016 роках, а також постійні спроби втручання в роботу залізниці та систем зв'язку під час повномасштабного вторгнення, підтверджують необхідність створення галузевих центрів реагування на кіберінциденти (Sectorial CERT), інтегрованих до загальнонаціональної системи. Такі центри вже функціонують в енергетиці та фінансовому секторі, однак потребують подальшого розвитку та стандартизації процедур [7].

Варто також підкреслити важливість міжнародної співпраці у формуванні національної кіберстійкості. Жодна держава, навіть найбільш технологічно розвинена, не здатна самостійно протистояти всім кіберзагрозам через їх транскордонний характер. Обмін інформацією про вразливості, індикатори компрометації та тактики зловмисників, спільні навчання та координація реагування на масштабні інциденти є критично важливими елементами сучасної архітектури кібербезпеки [20; 38]. Для України така співпраця з партнерами з НАТО, ЄС та США дозволяє не лише отримувати доступ до передових технологій та аналітики, а й інтегрувати національну систему захисту до глобальних механізмів колективної безпеки [27; 45].

Нарешті, важливо розуміти, що кібербезпека не є статичним станом, а динамічним процесом постійного управління ризиками. Жодна система не може бути абсолютно захищеною, тому ключовим показником спроможності держави є її здатність швидко відновлювати функціонування критичних сервісів після успішної атаки – так звана кіберстійкість (cyber resilience) [47]. Це передбачає не лише наявність технічних засобів резервування та відновлення, а й розроблені та відпрацьовані на практиці процедури реагування, чіткий розподіл ролей між відповідальними органами, а також регулярне тестування планів дій у надзвичайних ситуаціях через навчання та симуляції [7].

Таким чином, кібербезпека є фундаментальною умовою існування сучасної держави. Виходячи далеко за межі технічних аспектів, вона інтегрує в собі політичну стабільність, економічне процвітання та військову міць. Для України побудова ефективної системи кіберзахисту є запорукою збереження державного суверенітету в умовах гібридної агресії [40]. Отже, кібербезпека постає не просто як технічний додаток до системи національної безпеки, а як її невід'ємне ядро, що визначає життєздатність нації в епоху інформаційних воєн.

1.2 Політичні чинники формування державної політики у сфері кібербезпеки

Політичні чинники відіграють фундаментальну роль у структуруванні державної політики у сфері кібербезпеки, оскільки саме вони визначають стратегічну спрямованість, вибір інструментарію та ієрархію пріоритетів у межах національної оборонної парадигми [10; 23]. Протягом останнього десятиліття питання захисту цифрового простору зазнали кардинальної трансформації, перетворившись із вузькоспеціалізованої технічної проблеми на наріжний камінь національної безпеки, економічної стійкості та сучасної міжнародної дипломатії [9, с. 233; 33].

Реакція державних інституцій на виклики в цифровому просторі ніколи не є суто технічним процесом, оскільки вона значною мірою детермінована суб'єктивним сприйняттям та інтерпретацією загроз політичними елітами, бюрократичним апаратом та медійним дискурсом [21]. Резонансні кіберінциденти відіграють роль критичних каталізаторів, що здатні миттєво трансформувати суспільну свідомість і змусити державну машину до екстреної мобілізації ресурсів [25]. Аналіз подій останнього десятиліття переконливо доводить, як масштабні кампанії з втручання у виборчі процеси підірвали традиційну довіру до демократичних інститутів. Руйнівні операції, пов'язані з вірусами WannaCry та NotPetya, стали моментом істини для глобальної фінансової та енергетичної систем [35].

Кіберпростір у сучасних міжнародних відносинах остаточно утвердився як

арена міждержавного протистояння та ефективний інструмент реалізації зовнішньої політики [16; 30]. Державні інституції все активніше використовують кіберзасоби для досягнення розвідувальних цілей, здійснення політичного тиску на опонентів або цілеспрямованого руйнування економічного потенціалу супротивника без перетину фізичних кордонів [8, с. 21]. Політичні вибори в цій площині стосуються критичних питань: чи варто розвивати виключно оборонно-орієнтовані кіберпідрозділи, чи слід будувати активні системи стримування, здатні на асиметричну відповідь [27].

Одним із ключових політичних чинників є вибір моделі управління кібербезпекою, що визначає ієрархію та розподіл повноважень між цивільними відомствами, службами безпеки та змішаними структурами. Рішення про створення єдиного центру координації, його адміністративне підпорядкування та обсяг повноважень має безпосередній вплив на оперативність реагування та рівень демократичної підзвітності [5, с. 201]. Участь держави у багатосторонніх альянсах, таких як НАТО, додає ще один рівень політичних зобов'язань. Визнання кіберпростору доменом операцій на рівні Альянсу породжує потребу в сумісності національних систем захисту та готовності до колективних реакцій на кіберінциденти [27].

Таким чином, якість та послідовність державної політики у сфері кібербезпеки критично залежить від наявності та активності розвиненої експертної спільноти. Як слушно зазначає Т.А. Швець, найпоширенішою у світовій практиці є класифікація кіберзлочинів, закріплена у Конвенції Ради Європи про кіберзлочинність, яка поділяє їх на п'ять груп: злочини проти конфіденційності, цілісності та доступності комп'ютерних даних; злочини, пов'язані з використанням комп'ютера як знаряддя (комп'ютерне шахрайство та підробка); злочини, пов'язані з контентом (дитяча порнографія тощо); порушення авторських прав; а також расистські та ксенофобські дії, вчинені через комп'ютерні мережі [22, с. 10-11]. Технократична експертиза є тим містком, що дозволяє трансформувати загальні політичні гасла у конкретні технічні стандарти та дієві оперативні процедури. На думку М.Т. Гаврильціва, забезпечення інформаційної безпеки завдяки послідовній реалізації чітко сформульованої національної інформаційної стратегії значною мірою може

сприяти досягненню успіху при вирішенні завдань у політичній, військово-політичній, соціальній, економічній та інших сферах державної діяльності, а втілення вдалої інформаційної політики здатне суттєво вплинути на розв'язання внутрішньополітичних, зовнішньополітичних і військових конфліктів» [5, с. 201]. Фінансовий аспект є матеріальним втіленням політичної волі: рівень державних інвестицій у кібероборону, модернізацію застарілих ІТ-систем та професійну підготовку кадрів відображає реальні пріоритети уряду [14, с. 21].

Відносини між державою та суспільством у площині кібербезпеки формуються під впливом рівня довіри населення до владних інститутів та чутливості до питань захисту фундаментальних прав людини [10, с. 28]. У демократичних суспільствах будь-які спроби запровадження нових інструментів масового моніторингу або розширення повноважень спецслужб зустрічають вимоги щодо прозорості й судового контролю. Пошук балансу між потребами колективної безпеки та недоторканністю індивідуальних прав є перманентним політичним процесом.

Сучасні цифрові інструменти мають безпосередній вплив на стабільність демократичних процедур, зокрема на виборчі процеси та формування суспільної думки [25]. Держава змушена реагувати на ризики, пов'язані з витоком конфіденційних даних виборців, маніпулятивними технологіями в соціальних мережах та таргетованою дезінформацією [46]. Ситуація ще більше ускладнюється в умовах збройних конфліктів, коли пріоритети політики миттєво зміщуються в бік максимальної мобілізації ресурсів. Досвід України у 2022–2025 роках є найбільш показовим: безпрецедентна інтеграція зусиль цивільних та військових структур стала основою для вироблення нових підходів до кіберзахисту.

Атрибуція кіберінцидентів, тобто публічне встановлення винної сторони, є одним із найпотужніших дипломатичних інструментів сучасності. Це не просто технічний висновок, а серйозний політичний акт, який вимагає наявності неспростовних доказів та готовності уряду до погіршення двосторонніх відносин

[30]. Політичні наслідки офіційної атрибуції можуть включати запровадження економічних санкцій, висилання дипломатів або звернення до міжнародних судових інстанцій [40].

Важливим політичним чинником, який часто залишається поза увагою дослідників, є роль політичної культури та історичної пам'яті у формуванні ставлення до кібербезпеки. У державах із тривалим досвідом гібридних атак, як-от Україна, кібербезпека сприймається суспільством як невід'ємна складова національної оборони, а не як суто технічне питання. Це створює політичний запит на посилення кіберспроможностей та легітимізує виділення значних бюджетних ресурсів на ці цілі [21]. Натомість у країнах, які не зазнавали масштабних кібератак на критичну інфраструктуру, суспільний тиск на політиків щодо інвестицій у кібербезпеку значно нижчий, що може призводити до хронічного недофінансування цієї сфери [25].

Політична воля до міжнародної співпраці є окремим вагомим чинником, що визначає ефективність національної кіберполітики. У світі, де кіберзагрози не визнають державних кордонів, ізоляціонізм у цій сфері є апріорі провальною стратегією [30]. Політичне керівництво держави має ухвалювати рішення про приєднання до міжнародних механізмів обміну інформацією, участь у спільних навчаннях та узгодження національних стандартів із міжнародними. Приєднання України до Об'єднаного центру передових технологій з кібероборони НАТО (NATO CCDCOE) у 2023 році стало результатом саме політичного рішення на найвищому рівні, яке відкрило доступ до унікальних аналітичних ресурсів та програм підготовки фахівців [45]. Без такої політичної волі навіть найдосконаліші технічні рішення залишаються локальними та малоефективними проти скоординованих транскордонних атак [37].

Внутрішньополітична конкуренція також суттєво впливає на формування державної політики у сфері кібербезпеки. У країнах із високим рівнем політичної поляризації питання кібербезпеки нерідко стають об'єктом політичних спекуляцій та міжпартійної боротьби. Опозиційні сили можуть звинувачувати владу в недостатньому захисті цифрових кордонів, водночас блокуючи

законопроєкти, що передбачають розширення повноважень спецслужб у кіберпросторі через побоювання щодо їх використання для політичного переслідування [46]. В Україні, попри політичну конкуренцію, у сфері кібербезпеки з початку повномасштабного вторгнення спостерігається безпрецедентний консенсус, оскільки загроза з боку держави-агресора визнається всіма політичними силами як екзистенційна [16].

Чинник політичного лідерства – особистої позиції президента, прем'єр-міністра та ключових міністрів – часто стає вирішальним у моменти криз. Політичний лідер, який розуміє природу кіберзагроз та здатний комунікувати їхню важливість для суспільства, може суттєво прискорити ухвалення необхідних рішень. І навпаки, брак розуміння на найвищому рівні призводить до того, що кібербезпека залишається на периферії державної політики, а профільні відомства недоотримують фінансування та політичної підтримки. В Україні створення Національного координаційного центру кібербезпеки при РНБО та регулярний розгляд питань кіберзахисту на засіданнях Ради національної безпеки і оборони свідчать про високий рівень уваги до цієї сфери з боку вищого політичного керівництва.

Політичний вимір має також питання кіберосвіти та підвищення кібергігієни населення. Держава ухвалює політичне рішення про те, чи включати кібербезпеку до шкільних програм, чи створювати державні центри перепідготовки для дорослого населення, чи обмежитися добровільними ініціативами приватного сектору [20, с. 156]. В Україні ухвалено рішення про запровадження обов'язкових курсів кібергігієни для державних службовців та працівників критичної інфраструктури, що є прямим результатом політичної волі керівництва країни. Цей вибір відображає розуміння того, що людина є найвразливішою ланкою в будь-якій системі захисту, а інвестиції в людський капітал є не менш важливими, ніж закупівля новітніх технологічних рішень.

Важливим чинником є також ставлення політичних еліт до державно-приватного партнерства у сфері кібербезпеки. Переважна більшість критичної інфраструктури (енергетика, фінанси, транспорт, зв'язок) перебуває у приватній

власності або під контролем бізнесу. Тому без активної участі приватного сектору неможливо створити ефективну систему кіберзахисту національного масштабу [42]. Політичне рішення про те, які стимули створити для бізнесу (податкові пільги, зниження адміністративного тиску, захист від надмірної звітності), безпосередньо впливає на рівень захищеності приватних об'єктів критичної інфраструктури. Український досвід створення платформи MISP та залучення до неї приватних компаній свідчить про усвідомлення важливості такого партнерства, однак потенціал його розширення залишається значним [47].

Не менш важливим політичним чинником є здатність держави протидіяти дезінформації та інформаційно-психологічним операціям, які супроводжують кібератаки. Російська гібридна війна проти України продемонструвала, що кібератаки майже завжди поєднуються з масованими кампаніями дезінформації, спрямованими на посів паніки, дискредитацію влади та підрив довіри до державних інститутів [41; 46]. Політичне керівництво має ухвалювати рішення про те, як саме комунікувати з населенням про кіберінциденти: чи варто розкривати всю інформацію (ризикуючи спричинити паніку), чи обмежувати її (ризикуючи звинуваченнями в приховуванні). Україна обрала стратегію відносної відкритості, регулярно звітуючи про кіберінциденти через офіційні канали Держспецзв'язку та CERT-UA, що дозволило зберегти довіру громадян та міжнародних партнерів.

Нарешті, важливим чинником є політичний вибір щодо співвідношення між безпековими заходами та захистом прав людини. Розширення повноважень спецслужб у кіберпросторі, запровадження систем масового моніторингу, зберігання даних про користувачів – усе це створює ризики для приватності та свободи вираження поглядів [10, с. 28]. Політики мають знаходити баланс між необхідністю захисту національної безпеки та дотриманням демократичних стандартів. В Україні в умовах воєнного стану цей баланс тимчасово зміщений у бік безпекових заходів, що передбачено Конституцією та законами України.

Однак навіть у цих умовах зберігається судовий контроль та парламентський нагляд за діяльністю правоохоронних органів у кіберпросторі.

Таким чином, політичні чинники формування державної політики у сфері кібербезпеки виявилися надзвичайно багатовимірними. Вони охоплюють складний процес інтерпретації загроз, вибудовування ефективної інституційної архітектури та забезпечення сталого фінансування. Державна політика у цій сфері залишатиметься динамічним балансом між потребою в максимальній безпеці, прагненням до економічної інноваційності та захистом прав громадян.

1.3 Нормативно-правові засади забезпечення кібербезпеки в Україні

Нормативно-правове регулювання кібербезпеки в Україні пройшло значний шлях розвитку – від фрагментарних актів початку 2010-х років до комплексної багаторівневої системи, що охоплює закони, стратегії, доктрини та підзаконні акти. Правове забезпечення кібербезпеки є необхідною передумовою функціонування інституційної архітектури та ефективної протидії загрозам у цифровому просторі [9, с. 234].

Фундаментальною основою для формування політики кібербезпеки є Конституція України, яка гарантує право на інформацію, недоторканність приватного життя та визначає обов'язок держави забезпечувати інформаційну безпеку. Як зазначає А.П. Ряполов, нормативно-правове регулювання інформаційної безпеки в Україні базується на системному підході, що охоплює як стратегічне бачення національної безпеки, так і конкретні правові інструменти. Загальні засади такого регулювання формуються в межах Конституції України, законів, указів Президента, рішень РНБО, а також міжнародних договорів, ратифікованих Верховною Радою України. Зокрема, стаття 34 Конституції проголошує свободу думки і слова та вільний доступ до інформації, а стаття 17 закріплює обов'язок держави захищати національні інтереси [18, с. 89].

Фундаментальною основою для формування політики кібербезпеки є Конституція України, яка гарантує право на інформацію, недоторканність приватного життя та визначає обов'язок держави забезпечувати інформаційну

безпеку. На конституційному рівні закріплено принципи, які є базовими для подальшого галузевого регулювання.

Ключовим спеціалізованим законом є Закон України «Про основні засади забезпечення кібербезпеки України» (прийнятий 5 жовтня 2017 року, зі змінами, внесеними згідно із Законами № 1907-IX від 18.11.2021 та № 2595-IX від 29.07.2022) [1]. Цей закон визначає:

- організаційно-правові засади забезпечення кібербезпеки;
- повноваження та відповідальність суб'єктів забезпечення кібербезпеки;
- основні вимоги до системи управління кібербезпекою;
- порядок реагування на кіберінциденти та кібератаки;
- правовий статус національної команди реагування CERT-UA.

Закон закріпив створення Національної системи кібербезпеки, до якої входять: Рада національної безпеки і оборони України (координаційний орган), Служба безпеки України (контррозвідувальна діяльність), Державна служба спеціонального зв'язку та захисту інформації (технічний захист та CERT-UA), Національна поліція (розслідування кіберзлочинів), Міністерство оборони (воєнна складова), інші центральні органи виконавчої влади [5, с. 202; 1].

Важливе значення має також Закон України «Про інформацію», Закон України «Про захист інформації в інформаційно-комунікаційних системах» та Закон України «Про електронні довірчі послуги», які створюють правові рамки для функціонування цифрового середовища та захисту даних [9, с. 233].

Системоутворюючим документом є Стратегія кібербезпеки України, затверджена Указом Президента України № 96/2016 від 15 березня 2016 року [3]. Ця стратегія заклала основи національної політики у сфері кібербезпеки, визначила пріоритети створення Національної системи кібербезпеки та започаткувала міжвідомчу координацію.

Оновлена Стратегія кібербезпеки України була затверджена Указом Президента України № 447/2021 від 26 серпня 2021 року на підставі рішення Ради національної безпеки і оборони [2]. Нова стратегія врахувала досвід протидії кіберзагрозам у 2016–2021 роках, зокрема атаки на енергосистему 2015 року та кампанію NotPetya 2017 року [35

]. Документ визначив такі пріоритети:

- розвиток спроможностей захисту критичної інфраструктури;
- підвищення рівня кіберстійкості державних органів та бізнесу;
- розбудова системи реагування на кіберінциденти;
- інтеграція до міжнародних механізмів кібербезпеки (NATO CCDCOE, ENISA, ЄС);
- розвиток людського капіталу та освіти у сфері кібербезпеки.

Важливим документом є також Воєнна доктрина України, яка визнає кіберпростір окремим доменом ведення воєнних дій, а також Стратегія національної безпеки України, затверджена Указом Президента України № 392/2020 від 14 вересня 2020 року, що фіксує кібербезпеку як один із ключових напрямів забезпечення національної безпеки [8, с. 22].

Повномасштабне вторгнення Російської Федерації в Україну в лютому 2022 року призвело до безпрецедентних викликів у сфері кібербезпеки та вимагало оперативного реагування на законодавчому рівні [16; 47]. Було вжито такі ключові заходи:

1. Розширення повноважень Держспецзв'язку та CERT-UA. Відповідно до Закону України № 2595-IX від 29.07.2022, було розширено функції Державної служби спеціального зв'язку та захисту інформації України та її урядової команди CERT-UA щодо оперативного реагування на кіберінциденти, припинення кібератак та координації дій з міжнародними партнерами. Крім того, як наголошують Топчій та Бодунова, протягом першого місяця війни Верховна Рада оперативно ухвалила законопроєкти № 2137-IX та № 2149-IX, які вдосконалили процедури досудового розслідування кібератак «за гарячими слідами» та запровадили посилену кримінальну відповідальність за кіберзлочини, вчинені під час воєнного стану, зокрема доповнивши статтю 361 КК України частиною п'ятою [19, с. 667-668].

2. Посилення захисту критичної інфраструктури. Прийнято Закон України

«Про критичну інфраструктуру» (листопад 2021 року з подальшими змінами у 2022–2024 роках), який запровадив обов'язкові вимоги до кіберзахисту об'єктів енергетики, транспорту, зв'язку, фінансового сектору та інших стратегічних галузей. Закон також встановив персональну відповідальність керівників за неналежний рівень кібербезпеки.

3. Запровадження воєнного стану та особливих режимів кіберзахисту. Указами Президента України (зокрема № 64/2022 від 24.02.2022, № 133/2022 від 14.03.2022 та подальшими) було запроваджено особливі режими кіберзахисту державних інформаційних ресурсів, посилено моніторинг кіберпростору та обмежено доступ до окремих ресурсів, які використовувалися для дезінформації та кібератак.

4. Адаптація до європейського законодавства (NIS2, Cybersecurity Act). Україна розпочала процес гармонізації національного законодавства з Оновленою директивою ЄС з мережевої та інформаційної безпеки (NIS2) [27; 29]. Це передбачає:

- розширення переліку суб'єктів, на яких поширюються вимоги кібербезпеки;
- посилення вимог до управління ризиками в ланцюгах постачання;
- запровадження обов'язкової звітності про кіберінциденти;
- створення національних механізмів сертифікації ІТ-продуктів [22; 29].

5. Інтеграція до міжнародних центрів кібероборони. У березні 2023 року Україна стала повноправним членом Об'єднаного центру передових технологій з кібероборони НАТО (NATO CCDCOE) [45]. Це надало доступ до міжнародних навчань, аналітичних ресурсів та спільних операцій з атрибуції кібератак. Відповідно до політики НАТО, Альянс визнає кіберпростір доменом операцій (з 2016 року), а у 2021 році було затверджено Комплексну політику кібероборони, яка підтримує три основні завдання НАТО: стримування та оборону, запобігання кризам і управління ними, а також кооперативну безпеку. Важливо, що союзники визнали: вплив значних зловмисних сукупних кібероперацій за певних обставин може розглядатися як збройний напад, що дозволяє Північноатлантичній раді застосувати статтю 5 Вашингтонського договору [27].

6. Розвиток державно-приватного партнерства. У 2023–2025 роках було прийнято низку підзаконних актів, які врегулювали обмін інформацією про кіберзагрози між державою та бізнесом, зокрема через платформу MISP (Malware Information Sharing Platform) [17; 47]. CERT-UA у 2023 році опрацювала 2543 кіберінциденти, що свідчить про інтенсивність викликів та необхідність постійного вдосконалення правової бази [7].

7. Посилення кібердипломатії та санкційного механізму. У 2022–2025 роках Україна активно використовувала міжнародно-правові інструменти для притягнення до відповідальності державу-агресора за кібератаки. Спільно з ЄС та США було впроваджено санкції проти осіб та організацій, причетних до кібероперацій проти української критичної інфраструктури.

Попри значний прогрес, правове забезпечення кібербезпеки в Україні стикається з низкою викликів:

- недостатня імплементація окремих положень NIS2 через триваючу війну;
- потреба в удосконаленні механізмів притягнення до відповідальності за кіберзлочини в умовах воєнного стану;
- необхідність подальшої гармонізації законодавства з правом ЄС у контексті євроінтеграції [9, с. 235; 36];
- потреба в додатковому фінансуванні заходів кіберзахисту державних органів та критичної інфраструктури.

Водночас досвід 2022–2026 років засвідчив, що Україна здатна оперативно адаптувати нормативно-правову базу до нових викликів. Створення Національної системи кібербезпеки, інтеграція до міжнародних механізмів співпраці та системне оновлення законодавства дозволили державі витримати безпрецедентний тиск у кіберпросторі [47].

Таким чином, нормативно-правові засади забезпечення кібербезпеки в Україні становлять багаторівневу систему, що поєднує конституційні норми, спеціалізовані закони, стратегічні документи та підзаконні акти. В умовах повномасштабної війни ця система продемонструвала здатність до адаптації та розвитку, хоча потребує подальшого вдосконалення, зокрема в частині гармонізації з європейськими стандартами та посилення фінансового забезпечення.

Процес гармонізації українського законодавства з європейськими нормами у сфері кібербезпеки набув особливої інтенсивності після набуття чинності Угоди про асоціацію між Україною та Європейським Союзом. Ключовим орієнтиром для національного законотворця стала Оновлена директива ЄС з мережевої та інформаційної безпеки (NIS2) (Директива (ЄС) 2022/2555), яка встановлює жорсткіші вимоги до кіберстійкості порівняно з попередньою версією NIS [34; 36].

NIS2 розширює перелік секторів, що підпадають під регулювання, включно з

енергетикою, транспортом, банківськими та фінансовими послугами, охороною здоров'я, водопостачанням, цифровою інфраструктурою, а також секторами державного управління та космосу. Для України адаптація цих вимог означає необхідність перегляду національного переліку об'єктів критичної інфраструктури, що визначений Законом «Про критичну інфраструктуру» (2021 року зі змінами 2022–2024 років).

Ключові положення NIS2, які імплементуються в Україні, включають:

1. Посилення вимог до управління ризиками в ланцюгах постачання. Це передбачає обов'язкову оцінку безпеки програмного та апаратного забезпечення, що постачається від третіх сторін, а також впровадження механізмів контролю за субпідрядниками [29; 36]. В українському контексті це вимагає від операторів критичної інфраструктури перегляду договірних відносин з IT-постачальниками, особливо з тими, що мають корпоративні зв'язки з державою-агресором [41; 47].

2. Запровадження обов'язкової звітності про кіберінциденти. NIS2 встановлює чіткі часові рамки для інформування національних CERT- команд про значні інциденти: попереднє повідомлення протягом 24 годин, оновлене – протягом 72 годин, фінальний звіт – протягом одного місяця. В Україні цей механізм уже частково реалізовано через процедури CERT-UA, який у 2023 році опрацював 2543 інциденти, однак повна відповідність вимогам NIS2 потребує додаткового нормативного врегулювання.

3. Створення національних механізмів сертифікації IT-продуктів. NIS2 вимагає, щоб держави-члени ЄС запровадили схеми сертифікації кібербезпеки для критичних ІКТ-продуктів, послуг та процесів. Україна у цьому напрямі орієнтується на рамки, визначені Cybersecurity Act, який запровадив добровільну європейську схему сертифікації кібербезпеки (EUCS) для хмарних сервісів. Адаптація цих механізмів дозволить українським IT-компаніям отримувати європейські сертифікати безпеки, що є важливою умовою для інтеграції до цифрового ринку ЄС.

4. Посилення відповідальності керівного складу. NIS2 запроваджує персональну відповідальність керівників підприємств за недотримання вимог кібербезпеки, включаючи адміністративні та фінансові санкції. В Україні відповідні положення було включено до Закону «Про критичну інфраструктуру» та

внесено зміни до Кодексу України про адміністративні

правопорушення, що передбачають штрафи для посадових осіб за порушення вимог кіберзахисту [10].

Окрім NIS2, Україна активно імплементує положення Закону ЄС про кібербезпеку (Cybersecurity Act) (Регламент (ЄС) 2019/881), який створив мандат Агентства ЄС з кібербезпеки (ENISA) та запровадив рамки європейської сертифікації кібербезпеки [29]. Українські регулятори, зокрема Держспецзв'язку, співпрацюють з ENISA у питаннях обміну досвідом щодо розробки національних схем сертифікації [24]. Це дозволяє Україні не лише адаптувати європейські стандарти, а й брати участь у формуванні спільних підходів до кібербезпеки на рівні ЄС [9, с. 235].

Важливим аспектом гармонізації є також адаптація Рамкової програми кібербезпеки NIST CSF 2.0, яка, хоча й розроблена Національним інститутом стандартів і технологій США, широко використовується як міжнародний стандарт для управління кіберризиками [42]. NIST CSF 2.0 пропонує універсальну мову для опису стану кібербезпеки, що полегшує комунікацію між державними органами, бізнесом та міжнародними партнерами. Українські оператори критичної інфраструктури впроваджують цей фреймворк як доповнення до національних стандартів, що підвищує сумісність з європейськими та трансатлантичними партнерами [42].

Ефективність нормативно-правової бази кібербезпеки значною мірою залежить від дієвості механізмів притягнення до відповідальності за порушення у цій сфері. Українське законодавство передбачає кілька видів юридичної відповідальності за кіберправопорушення, однак їх практична реалізація стикається з низкою проблем [5, с. 202].

Кримінальна відповідальність за кіберзлочини передбачена розділом XVI Кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». До основних складів злочинів належать: несанкціоноване втручання в роботу комп'ютерів (ст. 361), створення та поширення шкідливого програмного забезпечення (ст. 361-1), несанкціонований збут або розповсюдження інформації з обмеженим доступом (ст. 361-2), порушення правил

експлуатації комп'ютерних мереж (ст. 363) [1]. Однак, як засвідчує практика протидії кібератакам з боку держави-агресора, застосування цих норм до суб'єктів, що діють з території Російської Федерації, є вкрай ускладненим через відсутність механізмів транскордонного переслідування та екстрадиції [28; 40].

Адміністративна відповідальність за порушення вимог кібербезпеки передбачена Кодексом України про адміністративні правопорушення. Згідно зі змінами, внесеними у 2022–2024 роках, передбачено штрафи для посадових осіб операторів критичної інфраструктури за: невиконання вимог щодо захисту інформації (ст. 188-19), неповідомлення про кіберінциденти (ст. 188-20), порушення вимог до організації роботи з інформацією з обмеженим доступом (ст. 188-21) [1]. Розміри штрафів поступово збільшувалися, однак вони все ще не досягають рівня, передбаченого NIS2 для держав-членів ЄС (до 10 млн євро або 2% річного глобального обороту).

Проблемним залишається питання цивільно-правової відповідальності за заподіяння шкоди внаслідок кібератак. Цивільний кодекс України передбачає відшкодування шкоди, завданої неправомірними діями, однак доведення причинно-наслідкового зв'язку між конкретною кібератакою та завданими збитками є вкрай складним завданням, особливо коли атаку здійснює державний суб'єкт [9, с. 233]. Ринок кіберстрахування в Україні перебуває на початковій стадії розвитку, хоча державна політика спрямована на його стимулювання через законодавчі ініціативи та податкові преференції [14, с. 19].

Окрему групу проблем становить відсутність уніфікованої практики притягнення до відповідальності за порушення, пов'язані з ланцюгами постачання програмного забезпечення. Інциденти, подібні до компрометації оновлення бухгалтерського ПЗ під час атаки NotPetya 2017 року, продемонстрували вразливість механізмів перевірки безпеки стороннього програмного забезпечення [35]. Нині в Україні триває робота над внесенням змін до Закону «Про захист інформації в інформаційно-комунікаційних системах» щодо посилення вимог до безпеки ланцюгів постачання, однак цей процес не завершено [1].

Воєнний стан, запроваджений в Україні з 24 лютого 2022 року, суттєво змінив пріоритети та інструменти нормативно-правового регулювання кібербезпеки. Указами Президента України (№ 64/2022, № 133/2022, № 259/2022,

№ 561/2023 та іншими) було запроваджено низку особливих режимів кіберзахисту, які дозволяють оперативно обмежувати доступ до окремих інформаційних ресурсів, пришвидшувати процедури реагування на кіберінциденти та залучати ресурси приватного сектору для захисту критичної інфраструктури [16].

Ключові нормативні зміни, запроваджені в умовах воєнного стану, включають:

1. Спрощення процедур набуття чинності рішень РНБО щодо кібербезпеки. Відповідно до Закону України «Про правовий режим воєнного стану», рішення РНБО про застосування обмежувальних заходів у кіберпросторі вводяться в дію указами Президента без попереднього розгляду Верховною Радою, що дозволяє пришвидшити реагування на загрози.

2. Розширення повноважень Держспецзв'язку щодо тимчасового блокування інтернет-ресурсів. За рішенням РНБО, введеним в дію Указом Президента

№ 133/2022, Державна служба спеціального зв'язку та захисту інформації отримала право у позасудовому порядку блокувати доступ до ресурсів, що використовуються для поширення дезінформації, координації кібератак або збору розвідувальних даних. Ці повноваження були використані для блокування низки проросійських ЗМІ та пропагандистських ресурсів у 2022–2023 роках [31].

3. Посилення вимог до кібергігієни для працівників критичної інфраструктури. Нормативно-правовими актами, прийнятими на виконання рішень РНБО, запроваджено обов'язкові програми підвищення кваліфікації та перевірки знань з кібербезпеки для працівників об'єктів

енергетики, транспорту, зв'язку та фінансового сектору [20, с. 159]. Порушення цих вимог тягне за собою адміністративну відповідальність посадових осіб [1].

4. Запровадження особливого порядку допуску до державної таємниці для фахівців з кібербезпеки. З метою пришвидшення залучення кваліфікованих кадрів до роботи в державних органах, відповідальних за кібербезпеку, було спрощено процедури оформлення допуску до державної таємниці для осіб, які мають відповідну кваліфікацію та досвід роботи [1].

Водночас запроваджені у зв'язку з воєнним станом обмеження викликають дискусії щодо їхньої відповідності європейським стандартам захисту прав людини. Зокрема, позасудове блокування інтернет-ресурсів потенційно може суперечити статті 10 Європейської конвенції з прав людини (свобода вираження поглядів) [46]. Однак практика Європейського суду з прав людини свідчить, що під час збройного конфлікту держави мають право на ширше тлумачення національної безпеки як підстави для обмеження окремих прав.

Незважаючи на значний прогрес у створенні нормативно-правових засад кібербезпеки, українське законодавство стикається з низкою системних проблем, які потребують вирішення в перспективі до 2030 року.

По-перше, залишається фрагментарним регулювання обміну інформацією про кіберзагрози між державним та приватним секторами. Хоча платформа MISP успішно функціонує, а CERT-UA опрацювала тисячі інцидентів, юридичні механізми захисту комерційної таємниці під час такого обміну потребують удосконалення. Бізнес часто побоюється розголошувати інформацію про інциденти через ризики репутаційних втрат та можливість використання цих даних у конкурентній боротьбі [42].

По-друге, необхідно завершити гармонізацію українського законодавства з NIS2 та Cybersecurity Act у повному обсязі. Особливу увагу слід приділити створенню національної схеми сертифікації кібербезпеки ІКТ-продуктів, яка б визнавалася в ЄС [29]. Це дозволить українським виробникам програмного забезпечення отримувати європейські сертифікати без додаткових процедур, що суттєво розширить їхні експортні можливості [9, с. 235].

По-третє, потребує вдосконалення механізм міжнародної правової допомоги у розслідуванні кіберзлочинів. Досвід атрибуції NotPetya та інших масштабних атак засвідчив, що без ефективної співпраці з правоохоронними органами інших держав притягнути винних до відповідальності практично неможливо [44]. Україна активно розвиває двосторонні угоди про обмін доказами у сфері кібербезпеки з партнерами, однак цей процес потребує прискорення [40].

По-четверте, важливим завданням є розвиток ринку кіберстрахування як інструменту управління ризиками. Наразі більшість українських компаній не

мають страхового покриття на випадок кібератак, що робить їх вразливими до фінансових втрат [14, с. 21]. Державна політика має передбачати створення стимулів для впровадження кіберстрахування, зокрема через податкові пільги для компаній, що мають відповідні поліси.

По-п'яте, потребує системного вирішення проблема кадрового забезпечення органів кібербезпеки. Незважаючи на наявність освітніх програм у провідних університетах, рівень оплати праці в державному секторі часто не конкурує з пропозиціями приватного бізнесу, що призводить до відтоку кваліфікованих кадрів [11]. Необхідне законодавче закріплення спеціальних умов оплати праці для фахівців з кібербезпеки, зайнятих у державних органах, аналогічних до умов для працівників інших силових структур [20, с. 159].

Таким чином, подальший розвиток нормативно-правової бази кібербезпеки України має бути спрямований на повну гармонізацію з європейським законодавством, посилення механізмів відповідальності за порушення вимог кібербезпеки, розвиток державно-приватного партнерства та підвищення привабливості державної служби для кваліфікованих фахівців. Вирішення цих завдань дозволить Україні не лише посилити власну кіберстійкість, а й стати повноцінним учасником європейського цифрового ринку.

РОЗДІЛ 2 ПОЛІТИЧНІ РИЗИКИ ТА ЗАГРОЗИ КІБЕРБЕЗПЕЦІ УКРАЇНИ В УМОВАХ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ

2.1 Державна стратегія кібербезпеки України та її політичні пріоритети

Адаптація до нових реалій війни та глобальних викликів XXI століття вимагає консолідації міжнародних зусиль і розвитку міждисциплінарних досліджень. Від технічних фахівців, що розробляють інноваційні протоколи захисту інформаційних систем, до юристів, які формують правові стандарти цифрового простору; від економістів, що оцінюють наслідки кібератак для бізнесу та держави, до психологів, що досліджують вплив кіберзагроз на свідомість людей. Усі вони повинні працювати як єдина команда. Лише така інтеграція знань та підходів дозволяє створити комплексну систему протидії викликам безмежного та динамічного кіберпростору [13, с. 8].

Державна стратегія кібербезпеки України 2021 року, введена в дію указом Президента №447/2021 на підставі рішення Ради національної безпеки і оборони, виступає ключовим державним документом, який визначає політичну логіку реагування на системні кіберзагрози і формує пріоритети державної політики в умовах тривалої російсько-української війни [2].

Оновлення стратегічного бачення в 2021 році стало реакцією на багаторічний набір кібератак і гібридних загроз, які кардинально змінили уявлення про природу і масштаби небезпек у кіберпросторі. Попередня версія стратегії, ухвалена у 2016 році, започаткувала створення базових інституцій і механізмів, проте накопичений досвід, в тому числі низка руйнівних операцій, потребував перегляду підходів до координації, законодавства і оперативних спроможностей. Оновлений документ узагальнює напрацювання і задає пріоритети для подальшого розвитку національної системи кібербезпеки [3].

У концептуальному вимірі Стратегія поєднує декілька взаємопов’язаних вимірів державної політики. Інституційний вимір спрямований на формування спеціалізованих органів координації і реагування, підвищення ролі апарату РНБО і створення національних механізмів для оперативної взаємодії. Правовий вимір

передбачає гармонізацію національного законодавства з міжнародними стандартами, встановлення процедур оцінки ризиків, визначення прав і обов'язків суб'єктів критичної інфраструктури, а також порядок обміну інформацією між державою й операторами ринку. Технічний вимір включає розвиток центру реагування, інструментів моніторингу, систем раннього виявлення і відновлення. Політика, яку фіксує документ, має бути водночас гнучкою й послідовною, щоб адаптуватися до швидкої зміни тактики супротивника.

Політичні пріоритети, закріплені у Стратегії, відображають прагнення держави побудувати стійку систему захисту критичної інфраструктури, підвищити готовність секторів економіки до відновлення після кіберінцидентів, інтегруватися у міжнародні механізми колективного реагування та зміцнити національний потенціал людських ресурсів. Захист критичної інфраструктури у стратегії розглядається не лише як технічне завдання, а й як політична мета: державна політика детально окреслює пріоритетні сектори, механізми регламентації і відповідальності операторів, а також підходи до аудиту й сертифікації. Законодавчі ініціативи в цій площині поєднуються з практичними заходами з підвищення кіберстійкості енергетики, транспорту, фінансів і державних сервісів [1].

В умовах повномасштабного вторгнення кіберпростір став невід'ємною складовою театру воєнних дій, де операції супроводжують і посилюють традиційну військову і інформаційну активність. Державна політика у відповідь трансформувалася у режимі безперервної мобілізації ресурсів: одночасно здійснюється підвищення оборонних спроможностей, нарощування розвідувальних можливостей і зміцнення захисту держсервісів та приватних операторів. У такій ситуації ключовим політичним пріоритетом є координація міжвідомчих зусиль, що дозволяє оперативно розподіляти завдання, уникати дублювання ресурсів і забезпечувати швидке відновлення критичних сервісів під час інцидентів.

Історичний досвід останнього десятиліття, зокрема масштабні інциденти з руйнівним потенціалом, дав підстави для політичних висновків щодо характеру загроз. Значна кібератака 2017 року, відома як NotPetya, була спрямована на ключову інфраструктуру України, але швидко набула глобального масштабу.

Використовуючи шкідливе програмне забезпечення під виглядом оновлення бухгалтерського софту, операція мала на меті дестабілізацію державних установ та бізнес-сектора, що призвело до паралізації фінансових систем, енергетичних компаній та логістичних вузлів. Ця подія продемонструвала здатність кібератак завдавати системних економічних збитків, виходячи далеко за межі суто ІТ-пошкоджень, і спричинила посилення волі до реформ та інституційних трансформацій у сфері кібербезпеки. Аналіз таких подій вплинув на активізацію заходів з підвищення стійкості й на створення процедур забезпечення доказової бази для міжнародних політико-правових реакцій [35].

Міжнародна співпраця становить окремий критичний політичний пріоритет. Україна послідовно інтегрується у міжнародні структури, що забезпечують обмін досвідом, участь у багатонаціональних навчаннях і доступ до аналітичної підтримки. Тісні зв'язки з партнерами, зокрема з США, ЄС та НАТО, посилюють спроможності України щодо атрибуції кібератак [37; 45]. Приєднання до NATO CCDCOE у 2023 році підвищило здатність держави не лише реагувати, а й формувати політику на міжнародному рівні [45].

Політика розвитку людського капіталу і науково-технічної бази є фундаментальним довгостроковим пріоритетом у сфері зміцнення національної безпеки та захисту цифрового суверенітету України [4, с. 199; 8, с. 22]. Освітні ініціативи, які впроваджуються на державному рівні через цільове оновлення університетських програм та запуск спеціалізованих курсів, програми підвищення кваліфікації для працівників державних органів, а також стратегічна співпраця з науковими інституціями, такими як Державна наукова установа «Інститут інформації, безпеки і права НАПрН України», безпосередньо спрямовані на системне формування професійного експертного середовища, спроможного оперативно та ефективно працювати з сучасними складними загрозами в інформаційному просторі [7; 20, с. 159]. Політичний вибір інвестувати в людські ресурси супроводжується комплексними заходами щодо всебічної підтримки вітчизняних наукових досліджень та прискореного розвитку національних технологічних рішень, що кардинально зменшує технологічну залежність держави від зовнішніх постачальників програмного забезпечення, нівелює загрози компрометації ланцюжків постачань і суттєво посилює національний суверенітет

у цифровій сфері [9, с. 234; 24]. Яскравим прикладом такої науково-технічної модернізації та підготовки кадрів стало повноправне приєднання України до Об'єднаного центру передових технологій з кібероборони НАТО (NATO CCDCOE), що відкрило доступ до унікальних практичних навчань та передового міжнародного досвіду для українських фахівців [45]. Практичне втілення цієї стратегії дозволяє протидіяти агресивним інформаційно-психологічним операціям та гібридним сурогатним методам війни, які систематично застосовуються проти нашої держави.

Політика взаємодії з приватним сектором та індустрією інновацій у сучасних умовах ґрунтується на засадах рівноправного партнерства, державно-приватного діалогу та стимулюванні високої юридичної і технічної відповідальності операторів об'єктів критичної інфраструктури, що закріплено на законодавчому рівні [5, с. 201; 1]. Держава не лише жорстко формує обов'язкові стандарти та нормативні вимоги, але й активно пропонує сучасні сервісні моделі взаємовигідної співпраці [1; 2]. Серед них особливе місце посідає автоматизований обмін телеметрією та даними про кіберзагрози, регулярні спільні міжвідомчі навчання, стандартизовані процедури негайного інформування про виявлені інциденти, а також гнучкі механізми взаємодопомоги у кризових ситуаціях [7; 17]. Прикладом такої успішної сервісної взаємодії є розгортання та функціонування урядовою командою CERT-UA спеціалізованої платформи MISP, яка дозволяє державі та приватному бізнесу в реальному часі обмінюватися індикаторами компрометації для випередження потенційних атак [17]. Як зазначається у звіті, «українська кібербезпека є спільними зусиллями уряду, приватного сектору та громадянського суспільства. Співпраця з партнерами та ефективна взаємодія між державними структурами, IT-спільнотою та волонтерами сформували фундамент нашої кіберстійкості» [47, с. 15]. Ефективність цієї моделі підтверджується тим, що лише протягом 2023 року CERT-UA спільно з партнерами опрацювала 2543 реальні кіберінциденти [7]. Більше того, Україна активно імплементує світові та європейські підходи у цих процесах, адаптуючи положення Оновленої директиви ЄС з мережевої та інформаційної безпеки (NIS2) та рамкові засади кібербезпеки NIST CSF 2.0 для кращої координації між державним сектором та приватними компаніями [34; 36;

42]. Такий інтегрований підхід чітко визнає, що стійка та ефективна національна спроможність у сфері кібербезпеки є абсолютно неможливою без проактивної участі приватного бізнесу у створенні загального високого рівня захищеності всього суспільства.

У нормативно-правовому полі політичні пріоритети орієнтовані на гармонізацію вітчизняних стандартів із практиками ЄС і НАТО, розвиток законодавства щодо критичної інфраструктури, захисту персональних даних та процедурного забезпечення реагування на інциденти. Законодавча модернізація має політичний характер, оскільки визначає рамки діяльності держави та приватних акторів, захищаючи при цьому права громадян і забезпечуючи прозорість процедур. Це важлива передумова для довгострокової інтеграції у міжнародні формати взаємодії [1].

Згідно з підходами НАТО, кіберзагрози не визнають державних кордонів, тому Альянс взаємодіє з партнерами, включаючи ЄС, ООН та ОБСЄ, на основі спільних цінностей та підходів до кібероборони. Російська війна проти України продемонструвала, що кібероперації є невід'ємною рисою сучасного конфлікту, а Росія посилила свої гібридні дії проти союзників НАТО, включаючи зловмисну кібердіяльність [27].

Питання атрибуції і відповідальності у кіберпросторі отримали політичне значення: спроможність встановити джерело атаки і надати переконливі докази має наслідки для дипломатичних ініціатив і санкційних політик. Тому політика передбачає поєднання технічної експертизи з правовим супроводом та міжнародною кооперацією, що дозволяє перетворювати технічні висновки на юридично значимі аргументи у міжнародних процесах [35].

Політика розвитку кібердипломатії та публічної дипломатії відіграє критично важливу роль у системі захисту суверенітету та просуванні геополітичних інтересів України на міжнародній арені. Чітка та аргументована комунікація на світовому рівні щодо характеру, масштабів та специфіки гібридних загроз, постійна демонстрація високої спроможності державних органів оперативно відповідати на руйнівні атакувальні дії супротивника, а також активне просування ініціатив щодо встановлення жорсткої міжнародно-правової відповідальності за протиправну поведінку у кіберпросторі забезпечують Україні

вагомий політичний вплив, посилюють її суб'єктність та гарантують стабільну підтримку з боку іноземних партнерів [10, с. 31; 33]. Важливим інструментом у цьому контексті виступає залучення міжнародних механізмів реагування, зокрема дипломатичного інструментарію ЄС (Cyber Diplomacy Toolbox), який передбачає спільну протидію зловмисній кібердіяльності за допомогою обмежувальних заходів [30]. Практична реалізація цієї політики спрямована на суттєве підсилення багатовекторної співпраці з ключовими міжнародними організаціями, такими як НАТО та Європейський Союз, авторитетною світовою академічною спільнотою та потужними приватними технологічними консорціумами [27; 37].

Сучасні політичні підходи до розбудови ринку страхування кіберризиків, всебічної підтримки вітчизняного IT-сектору та цілеспрямованого стимулювання передових наукових досліджень мають чітко виражений економічний вимір, оскільки системне посилення загального рівня кіберстійкості держави одночасно формує максимально сприятливі, прогнозовані та безпечні умови для розвитку інноваційних підприємств [14, с. 19]. Державні інвестиції в розробку національних технологічних рішень, створення гнучких механізмів фінансової підтримки підприємств для швидкого відновлення функціонування після деструктивних кіберінцидентів, а також законодавче сприяння формуванню повноцінного ринку кіберстрахування виступають ключовими елементами цілісної державної стратегії на стику безпеки та економічного зростання [2]. Україна у цій сфері орієнтується на провідні європейські та світові стандарти, адаптуючи вимоги Оновленої директиви ЄС з мережевої та інформаційної безпеки (NIS2) та положення Закону ЄС про кібербезпеку (Cybersecurity Act), які спрямовані на сертифікацію безпеки ІКТ-продуктів та підвищення стійкості ланцюжків постачань програмного забезпечення [29; 34; 36]. Впровадження таких інструментів, як Рамкова програма кібербезпеки NIST CSF 2.0, дозволяє українському бізнесу знизити фінансові ризики від потенційних кібератак [42; 37].

Фундаментальна політична логіка реалізації національної безпекової стратегії обов'язково передбачає створення дієвих, прозорих та чітко регламентованих механізмів контролю, відкритості та суворої підзвітності дій усіх уповноважених органів, що безпосередньо працюють у сфері кіберзахисту [1; 3]. Регулярний незалежний технічний та фінансовий аудит, системний

парламентський нагляд за діяльністю суб'єктів забезпечення кібербезпеки та регулярна публічна звітність профільних відомств, таких як Державна служба спеціального зв'язку та захисту інформації України або її аналітичні підрозділи, слугують надійними інструментами збереження стабільного балансу між інтересами державної безпеки та захистом основоположних прав і свобод громадян [7; 1; 47]. Забезпечення таких демократичних процедур має виключно політичну природу та є критично необхідним елементом для підтримки високого рівня довіри суспільства та легітимності будь-яких державних дій у сфері кіберзахисту, не дозволяючи перетворити інструменти безпеки на засоби цензури. Чітка нормативна фіксація прав та обов'язків державних органів, заснована на Законі України «Про основні засади забезпечення кібербезпеки України», гарантує, що заходи із захисту інформаційного простору здійснюються виключно в правовому полі, відповідають принципам верховенства права та захищають соціокультурні цінності українського суспільства [1].

Таким чином, Державна стратегія кібербезпеки 2021 року поєднує інституційну трансформацію, правову модернізацію, міжнародну інтеграцію, розвиток людського капіталу та технічні рішення як взаємодоповнювані елементи комплексної політики. Історичний досвід, оперативна статистика інцидентів та активна міжнародна співпраця підсилюють політичну аргументацію щодо необхідності послідовних інвестицій і координації дій, що у сукупності підвищують стійкість держави в кіберпросторі.

2.2. Зовнішні та внутрішні політичні загрози як інструмент гібридної війни

Під гібридною війною розуміється поєднання традиційних військових дій із комплексом невійськових засобів – інформаційних, кібернетичних, економічних, правових та прихованих операцій, спрямованих на досягнення політичних цілей при мінімізації прямого конфронтаційного ризику. Така стратегія будується на використанні вразливостей як усередині цільової держави, так і в міжнародному середовищі, де політичний ефект досягається через послаблення опору, підрив

довіри до інституцій і зміну зовнішньополітичних орієнтирів.

Історичні приклади демонструють, що гібридні інструменти використовувалися синхронно з військовими кроками для досягнення стратегічних результатів. Захоплення і подальша анексія кримського півострова в 2014 році супроводжувалися інформаційними операціями, операціями неоднозначної «сірозони» (підрозділи без розпізнавальних знаків, що отримали назву «little green men») і дипломатичними діями, які разом дозволили Кремлю змінити фактичний контроль без формального оголошення війни. Цей комплексний підхід був детально описаний у спеціалізованих аналізах як класичний приклад поєднання військової і невоєнної сили для швидкого встановлення контролю над територією. Як зазначає В.М. Гула, ще у 2013 році у так званій «Доктрині Герасимова» було сформульовано співвідношення військових та невійськових дій як 1:4, що передбачає переважання інформаційних, психологічних та інших невоєнних засобів над традиційними військовими. Це співвідношення успішно реалізується російською федерацією проти України з 2014 року [6, с. 36-37].

Один із центральних елементів зовнішньополітичних загроз – системні інформаційні кампанії та діяльність «фабрик тролів», які спрямовані на формування наративів за межами України з метою дискредитації української влади, послаблення підтримки з боку партнерів і розхитування європейської та трансатлантичної солідарності. М.Т. Гаврильців наголошує, що інформаційна складова є безумовним об'єктом маніпулювання в умовах гібридної війни, а складна політична ситуація, в якій перебуває Україна, постійне погіршення іміджу держави на міжнародній арені значною мірою зумовлені неналежним станом системи інформаційної безпеки» [5, с. 201]. Організовані мережі, пов’язані з інституціями російської влади або приватними структурами, систематично виробляли і поширювали дезінформацію у західних медіа та соціальних мережах ще з 2014 року, а досвід України часто розглядався в якості «поля випробувань» для подальших операцій за кордоном. Уперше широкомасштабні операції такого типу були задокументовані дослідниками і журналістськими розслідуваннями, які вказували на централізовану координацію пропагандистських меседжів і роботу мереж тролів, що працювали цілодобовими змінами та мали конкретні тактичні

завдання.

Кіберпростір став ще однією важливою ареною зовнішніх дій. З 2014 року й далі низка спрямованих кібероперацій завдавала відчутної шкоди фізичній інфраструктурі, державним інституціям і приватному сектору. Згідно з даними Держспецзв'язку, протягом 2022–2024 років в Україні діяло понад 200 російських хакерських груп, серед яких найактивнішими були UAC-0002 (Sandworm, підрозділ ГРУ), UAC-0010 (Gamaredon, пов'язаний з ФСБ), UAC-0004 (APT29) та UAC-0003 (Turla). Лише група UAC-0010 за три роки здійснила 829 інцидентів, що в середньому становить 23 інциденти на день» [47, с. 7, 11]. Прикладом є скоординовані атаки на енергетичну інфраструктуру в грудні 2015 року, коли злочинці зуміли вивести із ладу підстанції, спричинивши вимкнення світла в регіонах, а технічний і методичний рівень атак свідчив про ретельну підготовку і цілеспрямовану дію проти критичної інфраструктури. Розвиток у 2017 році шкідливого програмного забезпечення NotPetya, що почався з компрометації поширеного в Україні бухгалтерського ПЗ, спричинив глобальні наслідки для бізнесу і державних органів, підкресливши потенціал кібератак як засобу завдання системних економічних і політичних ударів. Ці інциденти підкреслюють, що кібероперації в рамках гібридної війни мають не лише локальний технічний ефект, а й значний політичний вплив, послаблюючи управлінську спроможність і підриваючи довіру громадян до держави.

Енергетика і торгівля виступають як інструменти зовнішнього тиску, що використовуються для досягнення політичних завдань. Росія регулярно застосовувала енергетичні важелі, зокрема маніпуляції поставками газу і ціновою політикою, які мали на меті створити економічний і політичний тиск на споживачів у Європі й Україні. Після широкомасштабного наступу 2022 року і подальших обмежень постачання енергоносіїв було очевидно, що енергетичні кроки Кремля виконують не лише економічні, а й геополітичні функції – вони впливають на політичні рішення держав і здатні підірвати єдність санкційного режиму або змусити переглянути позиції щодо підтримки України. Одночасно випадки диверсій на енергетичних інфраструктурах у міжнародних водах викликали складні політичні дебати і приклади щодо використання інфраструктури як цілі гібридної атаки. При цьому розслідування таких

інцидентів часто виявляються політично чутливими і неповними, що також є типовим компонентом гібридної стратегії [39].

Політичний вплив за межами України включав і складні операції спрямовані на західні аудиторії:

1. розповсюдження наративів, що підривають підтримку України серед громадян і законодавців у країнах-партнерах;
2. маніпуляції з метою затримання прийняття допоміжних рішень у парламентах;
3. залучення мереж проксі-акторів і маргінальних груп, які продукують «контрнарративи». Такі інформаційні кампанії були спрямовані саме на ослаблення політичної волі партнерів, а їхня мета полягала в тому, щоб перетворити міжнародну підтримку України на питання внутрішньої політики держав-донорів [46].

Внутрішні політичні загрози, як інструмент гібридної війни, мають визначальне значення, бо експлуатують внутрішні слабкості суспільства і державних інституцій. Серед таких загроз – проникнення агентів впливу в політичні партії і парламентські структури, контроль або значний вплив на ключові медіаресурси, фінансування політичних сил, що просувають проросійську повістку, корупційні схеми, що дозволяють підривати державні рішення, а також створення правових «підкладок» для легітимації такого впливу. На практиці це виявлялося в придбанні телеканалів і медіаплатформ, що стали каналами трансляції проросійських наративів, і в процедурі застосування «м'яких» економічних важелів (наприклад, незаконна торгівля на тимчасово окупованих територіях), що фінансово підживлювали прокремлівські мережі. Конкретний випадок – блокування в Україні низки телеканалів, пов’язаних із фігурами, яких пов’язували з проросійськими політичними колами, що викликав широкі дискусії щодо свободи слова та безпеки інформаційного простору. Цей приклад ілюструє, як системне фінансування і власність на медіа можуть бути використані як структурний інструмент для впливу на внутрішню політику в період гібридної агресії [31].

Інший аспект внутрішнього виміру гібридної війни – використання «правового» та «адміністративного» інструментарію для створення

правдоподібних пояснень зовнішньої інтервенції або для легітимації проросійських позицій. Масове надання російського громадянства або спрощене отримання паспортів для мешканців окремих районів Донбасу стало фактором, здатним створити юридичний привід для втручання під гаслом «захисту громадян», і тим самим модифікувати правові рамки суверенітету та міжнародного реагування. Ця «паспортізація» продемонструвала, як правові процедури можуть бути перетворені на стратегічний інструмент зовнішньої політики з прямими політичними наслідками для внутрішньої стабільності держави [38].

Маніпуляція інформаційним середовищем усередині країни включає не лише централізовані пропагандистські кампанії, а й організоване поширення фейків, підрив довіри до незалежних ЗМІ, створення або фінансування маргінальних інсайдерських видань і блогів, а також координацію бот-мереж для підсилення потрібних меседжів. У період передвиборчих кампаній такі впливи стають особливо помітними, оскільки змінюють виборчу поведінку через інформаційний шум, поляризацію суспільства та дискредитацію опонентів. Це часто супроводжується використанням технологій штучного створення контенту й автоматизації (наприклад, ботів і тролів), що підсилює їхню масштабність. Український медіапростір від часу 2014 року постійно зазнавав спроб системного впливу ззовні через контрольовані або симпатизуючі ресурси, що ускладнило інформаційну самоідентифікацію громадян [26].

Насильницькі й напівтаємні акти – від дискредитаційних операцій до фізичних нападів та вбивств – також використовувалися як елемент внутрішнього тиску. Основними складовими елементами інформаційної безпеки, як зазначає дослідник, є як забезпечення якісного інформування громадян і вільного доступу до різних джерел інформації, так і захист від негативних інформаційних впливів, що у сукупності мають сприяти цілісності суспільства» [5, с. 203]. Убивства і замахи на відомих журналістів, правозахисників чи активістів, навіть якщо їхня безпосередня вина не доведена, створюють ефект залякування й можуть призвести до самоцензури та відтоку критичних голосів із публічної сфери. Прикладом сталого тривожного тренду є серія нападів на журналістів і громадських діячів у різні роки, які кидали тінь на безпеку медійників і

посилювали ризики політичної демобілізації частин суспільства. Водночас такі інциденти часто стають інструментом для створення атмосфер нерозсудливості та підвищення суспільної поляризації. Залучення до цих операцій як локальних, так і зовнішніх агентів робить їх складною складовою внутрішньої загрози. Гібридні інструменти також включають використання приватних військових компаній і мереж проксі. Використання таких формувань дозволяє державі-актору діяти з більшою прихованістю й заперечувати пряму причетність, одночасно впливаючи на політичну ситуацію через присутність незаконних сил, дестабілізацію громадського порядку або через операції за кордоном, що спрямовані на легітимацію політичних режимів, які є союзниками агресора. З 2014 року по всьому спектру конфліктів, у яких фігурує росія, спостерігаються приклади використання приватних формувань для досягнення політичних завдань, що ускладнює ідентифікацію і юридичне реагування на такі операції [32].

Політична корупція і «захоплення» інституцій (процес, за якого державні установи, правоохоронні органи чи регулятори перестають діяти в інтересах суспільства та починають працювати на користь вузьких груп впливу) можуть виступати як довгостроковий механізм підриву стійкості держави. Коли впливові бізнес-елементи, що мають транскордонні зв’язки, отримують можливість домінувати над політичною системою через фінансові маніпуляції, вони здатні просувати рішення, що відповідають зовнішнім інтересам агресора, або блокувати реформи, які посилювали б стійкість держави.

Наслідки застосування зовнішніх і внутрішніх політичних загроз у формі гібридних дій є багатовимірними та мають системний вплив на стійкість держави. Аналіз наведених даних свідчить, що деструктивний вплив насамперед вражає легітимність державних інституцій, поступово підточуючи довіру громадян до органів влади та створюючи в суспільстві стійку атмосферу скептицизму. Це призводить до серйозних ускладнень у зовнішній політиці, оскільки держава втрачає спроможність формувати послідовний міжнародний курс і водночас втрачає внутрішній консенсус щодо стратегічних питань розвитку. Окрім політичної дестабілізації, гібридний тиск безпосередньо впливає на ресурсне забезпечення, змушуючи країну суттєво збільшувати витрати на безпеку та оборону, що неминуче відволікає критично важливі кошти від економічних і

соціальних програм. Кінцевим результатом такої стратегії є потенційна зміна рівня міжнародної підтримки, адже маніпуляції та дезінформація можуть негативно впливати на сприйняття держави її партнерами й донорами, послаблюючи її позиції на світовій арені. З точки зору довгострокової стійкості, систематичне використання таких методів проти політичної системи створює цикли вразливості, які важко виправити лише військовим чи короткостроковим політичним реагуванням [46].

Узагальнення практик російської гібридної війни проти України в період 2014–2025 років демонструє, що успіх таких операцій у значній мірі залежить від поєднання зовнішніх і внутрішніх інструментів: ззовні – інформаційні кампанії, кібератаки, енергетичний тиск, дипломатичні маніпуляції і використання проксі; всередині – контроль медіа, корупційні зв'язки, правова інструменталізація, дискредитація опонентів, насильство і створення «фальшивої нормальності». Розглянуті конкретні випадки – анексія Криму з 2014 року, атаки на енергосистему в 2015 році, масштабний NotPetya у 2017 році, інформаційні кампанії протягом 2014–2024 років, «паспортізація» Донбасу та роль проросійських медіа і олігархічних мереж у внутрішніх процесах – ілюструють складність і багатовимірність цих загроз.

Таким чином, детальний розгляд кожного з перелічених інструментів вказує, що політична війна у гібридній формі не обмежується одноразовими акціями: вона вимагає тривалої координації, ресурсного підживлення і адаптивної тактики, що змінюється відповідно до вразливостей цілі. Саме інтегроване поєднання зовнішніх і внутрішніх заходів створює «ефект синергії», коли окремі дії підсилюють одна одну, а кінцевим політичним результатом може стати зміна зовнішньополітичної орієнтації, ослаблення суспільної згуртованості або послаблення спроможності держави захищати свої інтереси.

2.3 Міжнародне політичне співробітництво України у сфері кібербезпеки та обміну даними

Зростання ролі кібербезпеки в державному й міжнародному порядку після

2014 року створило для України інтенсивну мережу двосторонніх і багатосторонніх політичних зв’язків, що поєднують інституційну підтримку, оперативний обмін даними та координацію заходів реагування. У період 2015–2025 років міжнародне співробітництво у цій сфері набуло кількох чітко виражених форм: інтеграція українських структур у євроатлантичні навчально-аналітичні центри, юридичне та технічне налагодження каналів обміну індикаторами компрометації, оперативні місії й мобілізація приватного сектору. Кожна з цих форм поєднує політичну легітимацію з практичною необхідністю захищати критичну інфраструктуру й державні сервіси під час широкомасштабної зовнішньої агресії.

Як зазначено на офіційному сайті НАТО, у 2023 році на Вільнюському саміті союзники схвалили нову концепцію посилення внеску кібероборони в загальний потенціал стримування та оборони Альянсу, а також запустили Віртуальну спроможність підтримки кіберінцидентів (VCISC) для підтримки національних заходів пом'якшення наслідків значних зловмисних кібероперацій. Крім того, на Вашингтонському саміті 2024 року лідери держав погодили створення Інтегрованого центру кібероборони НАТО для посилення захисту мереж, обізнаності про ситуацію та реалізації кіберпростору як операційного домену [27].

Інституційний вимір співпраці помітно проявився у входженні України до багатосторонніх платформ обміну знаннями та тренувань. Історичним кроком стало набуття Україною статусу країни-учасниці в НАТО Cooperative Cyber Defence Centre of Excellence (CCDCOE), що офіційно відбулося навесні 2023 року – це надало Києву доступ до постійних програм обміну знаннями, спільних навчань та аналітики, а також формалізувало участь українських фахівців у розробці спільних методик реагування. Наявність представництва в CCDCOE не тільки посилила політичну інтеграцію з Альянсом, але й створила додатковий канал для технічного обміну інформацією та координації у підготовці навчань і симуляцій [45].

Нормативно-правовою основою міжнародного співробітництва України у сфері кібербезпеки є передусім Закон України «Про основні засади забезпечення кібербезпеки України». Як зазначають А. Лисеюк та Т. Свінцицька, цей закон на

рівні принципів закріплює міжнародне співробітництво як один із ключових елементів національної системи кібербезпеки, що передбачає вироблення спільних підходів до протидії кіберзагрозам, консолідацію зусиль у розслідуванні кіберзлочинів та поглиблення співпраці з Європейським Союзом і НАТО, зокрема через участь у заходах ОБСЄ зі зміцнення довіри у кіберпросторі [12, с. 91].

Європейський вимір співпраці також включав як політико-дипломатичні інструменти, так і практичні ініціативи. Брюссель активізував механізми кібердипломатії (зокрема Cyber Diplomacy Toolbox) та проєкти підтримки кіберстійкості, а після лютого 2022 року ЄС мобілізував оперативні ресурси для посилення витривалості українських цифрових сервісів. Одним із прикладів стала ініціатива «EU Support to Strengthen Cyber Security in Ukraine», яка містила фінансування проєктів із підвищення стійкості державних сервісів та локальної інфраструктури, а також практичну координацію через двосторонні діалоги. Паралельно Євросоюз уперше в практичному контексті активував елементи спільної структури реагування – Cyber Rapid Response Teams (CRRT/PESCO) – для надання технічної допомоги українським операторам і державним органам під час кризових хвиль атак на початку масштабної агресії. Таким чином політична воля ЄС трансформувалася в технологічну і кадрову допомогу на місцях [30].

Практичний, технічний обмін даними між українськими структурами та партнерами здійснюється через стандартизовані платформи та формати. У національній системі реагування CERT-UA запроваджено та інтегровано систему обміну індикаторами компрометації на базі MISP (Malware Information Sharing Platform), яка дозволяє у режимі реального часу передавати IoC, тактики-техніки-процедури (TTP) та інші метадані між державними органами, військовими формуваннями, операторами критичної інфраструктури та міжнародними партнерами. На рівні законодавства і нормативу цей підхід закріплено в положеннях, що регламентують MISP-UA як інструмент координації обміну інформацією про кібератаки та технічні дані про ідентифікатори компрометації. Така архітектура забезпечує технічну інтероперабельність і політичний мандат на обмін оперативною інформацією [17; 47].

Співпраця зі США поєднувала дипломатичний, фінансовий та оперативно-технічний компоненти. Щорічні двосторонні кібердіалоги, меморандуми про

обмін інформацією й практичні програми підготовки дозволяли Україні отримувати не лише аналітичні продукти, але й фінансову допомогу на модернізацію засобів захисту; прикладом таких трансакцій є багаторічні пакети кібердопомоги, що рахувалися десятками мільйонів доларів у період після 2016 року і значно зросли після 2022 року. Окрім фінансування, американські установи – зокрема CISA і деякі підрозділи оборонного відомства – сприяли обміну методиками, інструментами для виявлення вразливостей та практиками проведення «hunt forward» операцій у партнерстві з українськими фахівцями. Ця підтримка була предметом офіційних звітів і прес-релізів в рамках спільних діалогів [37].

Політико-правовий аспект міжнародної взаємодії проявлявся і у формуванні механізмів стримування: ЄС та інші партнери посилювали практику адресних санкцій та дипломатичних заходів проти суб'єктів, причетних до злочинних кібероперацій; одночасно міжнародні документи про кібердипломатію й директиви з кіберстійкості створювали рамки для обміну доказовою базою та спільної публічної атрибуції інцидентів. Ці політичні інструменти зв'язували технічні дані з відповідними зовнішньополітичними відповідями, що надало операціям у кіберпросторі політичного ефекту й зробило їх частиною ширшої стратегії міжнародного тиску [40].

На фоні викликів бойових дій і постійного тиску з боку російських кібергруп, співпраця з міжнародними партнерами забезпечила Україні кілька важливих практичних результатів:

1. підвищення видимості атак через оперативний обмін індикаторами та аналітикою;
2. доступ до передових тренінгів і великих мультинаціональних навчань; можливість оперативно залучати диверсифіковані ресурси приватного сектору; фінансове підсилення модернізації кіберзахисту;
3. а також політико-дипломатичну підтримку у формі санкцій та міжнародної координації реагування. Ці результати демонструють, що для України кібербезпека перестала бути лише технічним питанням і трансформувалася в політичний і дипломатичний актив, який інструментально пов'язаний із зовнішньою підтримкою та партнерством [47].

Отже, міжнародне політичне співробітництво України у сфері кібербезпеки й обміну даними в 2015-2025 роках представляє собою багаторівневу мережу інституційних входжень, технічних платформ та оперативних зв’язків між державою, організаціями Альянсу, ЄС, урядами партнерів і приватними технологічними акторами. Ця мережа поєднує дипломатичну підтримку, фінансування, стандартизований обмін індикаторами й практичну координацію в режимі реального часу – і стала ключовим елементом здатності України протистояти системній кіберагресії.

ВИСНОВКИ

У ході дослідження встановлено, що кібербезпека в сучасних умовах є невід'ємною складовою національної безпеки держави та має виразний політичний вимір. Аналіз теоретико-політичних основ засвідчив, що кібербезпека виходить за межі суто технічного захисту інформаційних систем і охоплює комплекс інститутів, норм, стратегій і політичних рішень, спрямованих на забезпечення суверенітету, стійкості й безперервності функціонування держави. Залежність ключових суспільних процесів від цифрових технологій зумовлює те, що успішні кібератаки здатні мати системні політичні наслідки, включно з дестабілізацією управління, економічними втратами та підривом довіри громадян до влади.

У процесі виконання першого завдання було доведено, що місце кібербезпеки в системі національної безпеки визначається її інтегративним характером. Події, проаналізовані у роботі, зокрема атаки на енергетичну інфраструктуру України у 2015 році, показали, що кіберзагрози безпосередньо впливають на енергетичну, економічну та соціальну безпеку, а отже потребують політичних рішень на найвищому державному рівні. Кібербезпека стала складовою стратегічного стримування та одним із елементів оборонної політики, що підтверджується її інтеграцією до національних стратегій і доктрин.

Аналіз політичних чинників формування державної політики у сфері кібербезпеки дозволив встановити, що ключову роль у її розвитку відіграють інтерпретація загроз політичними елітами, міжнародне нормотворення, інституційні моделі управління та бюджетні пріоритети. Резонансні міжнародні та національні кіберінциденти, зокрема кампанія NotPetya 2017 року, стали каталізаторами політичних рішень щодо посилення нормативного регулювання, створення спеціалізованих органів і розвитку міжсекторної взаємодії. Було показано, що політика у сфері кібербезпеки формується під впливом зовнішньополітичних орієнтирів і прагнення інтеграції до європейських та євроатлантичних безпекових структур.

Результати аналізу Державної стратегії кібербезпеки України 2021 року підтвердили, що цей документ відіграє системоутворюючу роль у визначенні

політичних пріоритетів держави. Стратегія закріпила орієнтацію на захист критичної інфраструктури, міжвідомчу координацію, розвиток людського капіталу та міжнародне співробітництво. Практика реалізації стратегії в умовах повномасштабної війни засвідчила її адаптивність: розширення повноважень і спроможностей CERT-UA, активізація обміну інформацією з міжнародними партнерами та залучення технічної допомоги стали прикладами ефективного поєднання політичних і операційних рішень.

Дослідження зовнішніх і внутрішніх політичних загроз як інструментів гібридної війни дозволило встановити, що кіберпростір використовується для досягнення стратегічних цілей без прямого застосування військової сили. Кібероперації проти державних органів, кампанії дезінформації, втручання в інформаційні системи та спроби підриву виборчих процесів спрямовані на ослаблення політичної стабільності України. Аналіз прикладів гібридних дій у поєднанні з воєнними операціями підтвердив, що кіберзагрози є важливим елементом комплексного тиску на державу.

У межах аналізу міжнародного політичного співробітництва було встановлено, що інтеграція України до міжнародних механізмів обміну даними та спільного реагування суттєво підвищує її кіберстійкість. Співпраця з партнерами, участь у багатонаціональних навчаннях і доступ до аналітичних ресурсів сприяють підвищенню здатності держави до атрибуції кібератак і формування політико-дипломатичних відповідей. Практика міжнародної підтримки України після 2022 року стала підтвердженням того, що кібербезпека є важливим елементом сучасної системи колективної безпеки.

Узагальнюючи результати дослідження, можна стверджувати, що політичні аспекти кібербезпеки визначають ефективність протидії сучасним загрозам і формують основу національної стійкості України. Реальні приклади, наведені у роботі, підтверджують, що успішна кіберполітика потребує поєднання стратегічного бачення, інституційної спроможності та міжнародної взаємодії. Досягнення мети та виконання поставлених завдань дозволили комплексно розкрити політичну природу кіберзагроз і обґрунтувати ключову роль державної політики у забезпеченні безпеки України в кіберпросторі.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. Про основні засади забезпечення кібербезпеки України. Закон України із змінами, внесеними згідно із Законами № 1907-IX від 18.11.2021. URL: https://zakon.rada.gov.ua/laws/show/2163-19/ed20211215#Text

2. Указ Президента України №447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

3. Указ Президента України №96/2016. URL: https://www.president.gov.ua/documents/962016-19836

4. Виздрик В., Мельник О. Інформаційна безпека в Україні. Grail of Science. 2023. № 24. С. 196–202.

5. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий електронний журнал. 2020.

6. Гула В. М. Державна політика щодо інформаційної безпеки України : кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» : спец. 281 «Публічне управління та адміністрування» / В. М. Гула ; ЧНУ ім. Петра Могили. Миколаїв, 2023. 80 с. URL: https://krs.chmnu.edu.ua/jspui/handle/123456789/3009

7. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/uryadova-komanda-cert-ua-v-2023-roci-opracyuvala-2543-kiberincidenti

8. Залєвська І.І., Удренас Г.І. Інформаційна безпека в Україні в умовах російської військової агресії. Південно-український правничий часопис. 2022. №

9. Зуй В. В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. Правове забезпечення адміністративної реформи. 2022. Ч.1. №4. С. 231-235.

10. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. Політичні науки. 2019. № 1. Вип. 2. С. 27–32.

11. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права

НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. К., 2023.

12. Лисеюк А., Свінцицька Т. Розвиток міжнародного співробітництва у сфері кібербезпеки: нормативно-правові засади та перспективи. Право та інноваційне суспільство. 2024. № 2(23). С. 89-95. URL: https://apir.org.ua/lais/uk/article/view/45

13. Матеріали Міжнародної науково-практичноїконференції«Кібербезпека в сучасному світі: актуальні виклики» (м. Одеса, 28 листопада 2025 р.). Одеса, 2025. 287 с. URL: file:///C:/Users/user/Downloads/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0%20%D0%B2%20%D1%81%D1%83%D1%87%D0%B0%D1%81%D0%BD%D0%BE%D0%BC%D1%83%20%D1%81%D0%B2%D1%96%D1%82%D1%96%20_2025.pdf

14. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2018. № 1. С. 17–23.

15. Панченко О. Інформаційна безпека держави як елемент соціокультури. Аспекти публічного управління. 2020. № 1. С. 58–67.

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

17. Роз’яснення CERT-UA: платформа MISP, що це, як підключатися та які переваги. Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/faqs/roz-yasnennya-cert-ua-platforma-misp-sho-ce-yak-pidklyuchatisya-ta-yaki-perevagi

18. Ряполов А.П. Нормативно-правові основи інформаційної безпеки України в умовах гібридної агресії. Науковий вісник Ужгородського Національного Університету. 2025. № 89. Ч. 3. С. 87-91. URL: https://visnyk-pravo.uzhnu.edu.ua/article/view/336476/325112

19. Топчій В.В., Бодунова О.М. Проблемні питання забезпечення кібербезпеки в Україні. Аналітично-порівняльне правознавство. 2025. № 1. С. 665-669. URL: https://dspace.uzhnu.edu.ua/server/api/core/bitstreams/a07349dc-bda3-4b5e-bc8a-5093bee8d2d8/content

20. Уханова Н.С. Правова культура молоді в Україні. Інформація і право.

2019. № 2. С. 156–166.

21. Худолій А. Кібербезпека: сучасні виклики перед Україною. Acta de Historia & Politica Saeculum XXI. 2020. URL: https://www.researchgate.net/publication/342228040_Kiberbezpeka_sucasni_vikliki_pered_Ukrainou

22. Швець Т.А. Кіберзлочинність як виклик державній інформаційній політиці. Магістерська робота. Острог: Національний університет «Острозька академія», 2022. 88 с. URL: https://theses.oa.edu.ua/DATA/6551/%D0%A8%D0%B2%D0%B5%D1%86%D1%8C%20%D0%A2%D0%B5%D1%82%D1%8F%D0%BD%D0%B0%20%D0%90%D0%BD%D0%B0%D1%82%D0%BE%D0%BB%D1%96%D1%97%D0%B2%D0%BD%D0%B0.pdf

23. Ящук В.І. Роль та місце стратегії кібербезпеки України у забезпеченні інформаційної безпеки держави. (Стаття за матеріалами наукової конференції). Львів: Львівський державний університет безпеки життєдіяльності. URL: https://sci.ldubgd.edu.ua/bitstream/123456789/13824/1/1%20Yashchuk_monogr_rozdil13.pdf

24. Call for Feedback: Advancing Software Supply Chain Security together! Enisa. 2025. URL: https://www.enisa.europa.eu/

25. Cassidy C. A. Cybersecurity executive tapped to lead agency that protects voting systems. Apnews. 2025. URL: https://apnews.com/article/election-security-cybersecurity-cisa-director-05cc9b7ba56dfec954f3bfeb498cd524

26. Cyber and Information warfare in the Ukrainian conflict. CSS. 2018. URL: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/20181003_MB_HS_RUS-UKR%20V2_rev.pdf

27. Cyber defence. NATO. 2024. URL: https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

28. Cyber-Attack Against Ukrainian Critical Infrastructure. 2021. URL: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

29. Cybersecurity Act. URL: https://certification.enisa.europa.eu/about-eu-cyber-certification/eu-regulatory-context/cybersecurity-act_en

30. Delegations will find attached the Revised Implementing Guidelines of the Cyber Diplomacy Toolbox. 2023. URL: https://data.consilium.europa.eu/doc/document/ST-10289-2023-INIT/en/pdf

31. Dickinson P. Analysis: Ukraine bans Kremlin-linked TV channels. Atlantic Council. 2021. URL: https://www.atlanticcouncil.org/blogs/ukrainealert/analysis-ukraine-bans-kremlin-linked-tv-channels/

32. Foley E., Kaunert Ch. Russian Private Military and Ukraine: Hybrid Surrogate Warfare and Russian State Policy by Other Means. Central European Journal of International and Security Studies. 2022. № 16 (3). URL: https://cejiss.org/russian-private-military-and-ukraine-hybrid-surrogate-warfare-and-russian-state-policy-by-other-means

33. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. General Assembly. 2021. URL: https://dig.watch/wp-content/uploads/2022/08/UN-GGE-Report-2021.pdf

34. NIS2 Directive: securing network and information systems. EU. 2026. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

35. NotPetya: A Columbia University Case Study. SIPA. 2022. URL: https://www.sipa.columbia.edu/sites/default/files/2022-11/NotPetya%20Final.pdf

36. Pop F. et al. The NIS2 Directive: the Road Map to Strengthen Cybersecurity Across the EU. 2025. URL: https://www.eipa.eu/blog/the-nis2-directive-the-road-map-to-strengthen-cybersecurity-across-the-eu/

37. Proceedings of the 2023 U.S.-Ukraine Cyber Dialogue. 2023. URL: https://2021-2025.state.gov/proceedings-of-the-2023-u-s-ukraine-cyber-dialogue/?safe=1

38. Russia's "Passportisation" of the Donbas. SWP. 2020. URL: https://www.swp-berlin.org/10.18449/2020C41/

39. Russia's Use of the "Energy Weapon" in Europe. 2017. URL: https://www.bakerinstitute.org/research/russias-use-energy-weapon-europe

40. Sanctions adopted following Russia's military aggression against Ukraine. 2025. URL: https://finance.ec.europa.eu/eu-and-world/sanctions-restrictive-measures/sanctions-adopted-following-russias-military-aggression-against-ukraine_en

41. The hybrid war in Ukraine. 2022. URL: https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/

42. The NIST Cybersecurity Framework (CSF) 2.0. NIST. 2024. URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

43. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. 2018. URL: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

44. Uchill J. White House confirms NotPetya malware was Russian military operation. Axios. 2018. URL: https://www.axios.com/2018/02/15/white-house-confirms-notpetya-1518728781

45. Ukraine becomes a member of the NATO's Cooperative Cyber Defense Center of Excellence. RNBO. 2023. URL: https://www.rnbo.gov.ua/en/Diialnist/6335.html?PRINT=

46. Undermining Ukraine: How Russia widened its global information war in 2023. Atlantic Council. 2024. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/

47. War and Cyber: Three Years of Struggle and Lessons for Global Security. Analytical report. 2025. URL: https://cip.gov.ua/services/cm/api/attachment/download?id=69131