УДК 323:004.056:658 DOI 10.17721/2415-881X.2026.100.1.342–358

Фомін Іван Олександрович
Аспірант кафедри політології, соціології і культурології,
факультет соціально-гуманітарних наук і соціальних технологій
Харківський національний педагогічний університет
імені Г. С. Сковороди (м. Харків, Україна)
https://orcid.org/0009-0007-7593-9134
e-mail: bezpeka.khladik@gmail.com

ПОЛІТИЧНІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Резюме

У статті здійснено комплексний аналіз політичних механізмів та стратегічних рамок забезпечення інформаційної безпеки підприємств України в умовах гібридної війни. Актуальність дослідження зумовлена трансформацією загрозового середовища внаслідок масованої російської кіберагресії, яка формує принципово новий ландшафт ризиків для корпоративного сектору, що виходить за межі традиційних моделей кібербезпеки. У цьому контексті інформаційна безпека підприємств розглядається не як суто технічна проблема, а як невід'ємна складова національної кіберстійкості та цифрового суверенітету держави.

Особливу увагу приділено аналізу Національної стратегії кібербезпеки України (2021 — 2025) як основоположного документа, що закладає інституційне підґрунтя для багаторівневої системи захисту. Показано, що ефективність цієї системи безпосередньо корелює з якістю міжвідомчої координації між РНБО, ДССКЗІ, СБУ та Міністерством цифрової трансформації, а кіберстійкість підприємств є функцією не лише їхньої власної захищеності, а й загальнонаціональної архітектури управління інцидентами. Досліджено механізми залучення приватного сектору через законодавчі рамки, державно-приватні партнерства та галузеві CERT-центри.

Проаналізовано роль міжнародного співробітництва — Талліннського механізму, Резерву кібербезпеки ЄС, Фонду

кібербезпеки NL-UA — як незамінного компонента системи захисту. Водночас доведено, що тимчасове призупинення американської розвідувальної підтримки на початку 2025 року виявило реальний ризик стратегічної залежності та актуалізувало необхідність диверсифікації партнерств відповідно до принципу «нічого про Україну без України». Введено концепцію багаторівневої стійкості, що реалізується через взаємодію державних регуляторів, бізнесу та організацій громадянського суспільства.

У підсумку обґрунтовано тезу, що забезпечення інформаційної безпеки підприємств в умовах гібридної війни неможливе без інтеграції корпоративного захисту у єдину загальнонаціональну систему кіберстійкості. Підкреслено обмеженість суто технічних підходів до кіберзахисту за умов геополітичної нестабільності та наголошено на значенні інституційної координації, міжнародного партнерства та впровадження базових вимог безпеки (архітектура нульової довіри, багатофакторна автентифікація, постквантова криптографія) для забезпечення довгострокового цифрового суверенітету держави в умовах тривалої збройної агресії.

Ключові слова: інформаційна безпека; кібербезпека підприємств; гібридна війна; критична інформаційна інфраструктура; державно-приватне партнерство; кіберстійкість; цифровий суверенітет.

Вступ

Актуальність вивчення політичних механізмів забезпечення інформаційної безпеки підприємств в умовах гібридної війни зумовлена принциповою трансформацією загрозового середовища, пов'язаною з поєднанням кібератак, дезінформації та атак на ланцюги постачання. Гібридна війна формує специфічний тип загроз для корпоративного сектору, для якого характерними є системність ударів по критичній інфраструктурі, залежність підприємств від стану національних цифрових мереж та неможливість протидії загрозам виключно власними силами. За таких умов інформаційна безпека підприємств втрачає суто технічний характер і стає невід'ємною складовою національної кіберстійкості.

Вивчення цієї проблематики є особливо значущим з огляду на безпосередній зв'язок між ефективністю державних політичних механізмів та захищеністю корпоративного сектору. Неспроможність окремих підприємств самостійно протистояти геополітично вмотивованим кіберзагрозам зумовлює першочергову роль державних стратегій, міжвідомчої координації та міжнародних партнерств. У цьому контексті інформаційна безпека підприємств постає не лише як технічна, а як політична проблема, що потребує комплексного інституційного осмислення.

Досвід України 2022 — 2025 років ілюструє, що каскадний ефект атак на критичну інфраструктуру безпосередньо дестабілізує операційне

середовище бізнесу, тоді як ефективна відповідь можлива лише через інтеграцію корпоративного захисту у загальнонаціональну архітектуру кіберстійкості. Саме у цьому контексті політичні механізми постають як ключовий інструмент подолання розриву між задекларованими пріоритетами кібербезпеки та їхньою практичною реалізацією на рівні підприємств.

Метою цього дослідження є аналіз політичних механізмів і стратегічних рамок забезпечення інформаційної безпеки підприємств України в умовах гібридної війни у 2022 — 2025 роках та апробація моделі оцінки розривів між задекларованими пріоритетами кібербезпеки та їхньою практичною реалізацією на рівні корпоративного сектору. Така модель дозволяє не лише вивчати динаміку трансформації системи захисту підприємств під час активної фази збройного конфлікту, а й прогнозувати поствоєнні процеси відновлення та зміцнення цифрового суверенітету держави.

Дослідження спрямоване на виявлення ключових інституційних і нормативно-правових чинників інформаційної безпеки підприємств у кризових умовах, трансформацію загрозового середовища внаслідок гібридної агресії, оцінку адаптації механізмів кіберзахисту та визначення їхнього впливу на перспективи цифрової стійкості корпоративного сектору після завершення війни [1, с. 12-13; 2, с. 45-52; 3, с. 145; 4, с. 86-88; 5, с. 192].

Методи дослідження

Дослідження ґрунтується на поєднанні інституційного, порівняльно-правового та стратегічно-структурного аналізу, що забезпечує багатовимірне осмислення політичних механізмів інформаційної безпеки підприємств в умовах гібридної війни. Зокрема, такий підхід дає змогу розглядати кіберзахист корпоративного сектору у контексті трансформацій загрозового середовища, інституційної координації та міжнародного співробітництва. Інституційний підхід дозволяє виявити функціональні зв'язки між ключовими суб'єктами системи кібербезпеки — РНБО, ДССКЗІ, СБУ та Міністерством цифрової трансформації — і з'ясувати їхню роль у формуванні багаторівневої архітектури захисту підприємств. Порівняльно-правовий підхід використовується для аналізу відповідності національного законодавства міжнародним стандартам — директивам ЄС NIS2, DORA та рекомендаціям ENISA — в межах яких інформаційна безпека підприємств набуває форми системної регуляторної вимоги. Стратегічно-структурний підхід, доповнений кількісним аналізом даних про кібератаки та оцінкою ефективності міжнародних грантових програм, застосовується для виявлення розривів між задекларованими пріоритетами Національної стратегії кібербезпеки та їхньою практичною реалізацією на рівні корпоративного сектору. Дослідження спирається на поєднання інституційного, порівняльно-правового та стратегічно-структурного аналізу, аналізу нормативних документів — Конституції України, законів, указів Президента, стратегій

кібербезпеки — а також кількісного аналізу даних про кібератаки та оцінки ефективності грантових програм міжнародних партнерів. Така комбінація методів дозволяє не лише описати фактичний стан захисту підприємств, а й запропонувати аналітичний інструмент для подальших досліджень поствоєнної цифрової відбудови [2, с. 45-52; 6, с. 87-102; 4, с. 86-88].

Результати дослідження

У межах теоретичного осмислення інформаційної безпеки підприємств особливу увагу приділено трьом тематичним напрямам аналізу проблеми в умовах гібридної війни. Перший пов'язаний із нормативно-правовим і стратегічним виміром: Пашковський В. Ф. підкреслює, що ефективність інформаційної політики держави у протидії гібридним загрозам можлива лише за умови синергії «жорстких» (санкції, блокування ресурсів, регулювання медіа) та «м'яких» (стратегічні комунікації, фактчекінг) інструментів [1, с. 16]. В умовах гібридної війни пріоритет набуває не лише правове регулювання, а й інституційна координація між РНБО, Міністерством цифрової трансформації та ДССКЗІ, тоді як дискурсивні та комунікативні практики набувають особливої ваги для підтримання довіри бізнесу до державних механізмів захисту [7, с. 97].

Другий напрям зосереджений на загрозовому вимірі гібридної війни та її впливові на інформаційну безпеку підприємств. Ноференко А. показав, що механізми протидії російській інформаційній агресії поділяються на законодавчі та інституційні, причому серед вітчизняних інституційних механізмів ключову роль відіграють РНБО, кіберполіція та профільні міністерства [8, с. 72]. Радченко О. В. та Чмир Я. І. визначають гібридну війну як «якісно нову радикальну форму геополітичного конфлікту», де основною зброєю є інформація та інтернет-мережі, цілеспрямовані на зміну суспільної свідомості та інформаційне поневолення держави-мішені [9, с. 49]. Досвід України 2022 — 2025 рр. ілюструє феномен «каскадного кіберудару», коли атаки на критичну інфраструктуру — залізниці, енергомережі, фінансові системи — безпосередньо дестабілізують підприємницьке середовище [6, с. 89].

Третій напрям стосується взаємозв'язку інформаційної безпеки підприємств та зовнішнього виміру — міжнародного співробітництва й інтеграції в євроатлантичний безпековий простір. Дослідження такого взаємозв'язку [2, с. 49; 10, с. 86] демонструють, що державний інформаційний суверенітет у сучасних умовах технологічного розвитку невіддільний від безпеки корпоративних мереж і потребує комплексних методологічних засад на індивідуальному, організаційному та загальнодержавному рівнях. Пронін А. акцентує, що скоординовані кібератаки та інформаційні кампанії взаємно посилюють свій руйнівний вплив, тому системна відповідь має передбачати гармонізацію законодавства з директивами ЄС (NIS2, DORA,

ENISA) та інтеграцію механізмів захисту підприємств у єдиний євроатлантичний кіберпростір [11, с. 31].

Ключові категорії аналізу охоплюють інформаційну безпеку підприємств як стан захищеності цифрових активів, систем зв'язку та операційної інфраструктури організацій від кібератак і гібридних дестабілізуючих впливів; кіберстійкість як здатність підприємства виявляти загрози, адаптуватися до них та відновлювати операційну діяльність; критичну інформаційну інфраструктуру як сукупність систем, порушення функціонування яких може спричинити надзвичайну ситуацію в економіці або сфері національної безпеки. Гібридна загроза розглядається як стратегія, що поєднує кібератаки, дезінформацію, економічний тиск та диверсії задля дестабілізації держави-мішені без переходу до відкритої конвенційної війни [12, с. 7; 9, с. 49]. Інформаційний суверенітет визначається здатністю держави та підприємств самостійно контролювати власний інформаційний простір, протидіяти зовнішньому маніпулюванню та забезпечувати захист цифрових активів навіть в умовах активної збройної агресії. Державно-приватне партнерство у сфері кібербезпеки включає нормативно-правові, координаційні та технічні механізми взаємодії між державними органами та суб'єктами господарювання, що реалізуються через галузеві CERT, платформи обміну даними про загрози та спільні навчання [1, с. 19; 10, с. 85].

Ці три комплементарні напрями аналізу утворюють теоретичну основу для розуміння політичних механізмів, спрямованих на захист інформаційної безпеки українських підприємств в умовах гібридної загрози. Водночас розгляд цього питання вимагає детального аналізу того, як саме ці загрози матеріалізуються у площині конкретних суб'єктів господарювання та яким чином держава через систему політичних і правових механізмів протидіє їм.

Гібридна війна поєднує традиційні військові дії та невійськові тактики, такі як кібератаки, дезінформація, економічний тиск і саботаж, для дестабілізації держави-мішені. З 2014 року Росія застосовує ці методи проти України, включаючи «зелених чоловічків» у Криму, напади на енергомережі та дезінформаційні кампанії, створюючи каскадний ефект на бізнес-сектор та підприємства України під час традиційної війни після 2022 року.

Розуміння загроз в інформаційній безпеці є важливим для аналізу їхнього впливу на підприємства. У конфліктному середовищі інформаційна безпека забезпечує захист цифрових активів, комунікацій, фінансів і інфраструктури від кібератак та гібридної війни. Українські підприємства постійно зазнають атак з боку російських державних суб'єктів, зокрема понад тисячу атак на критичні системи у 2024 році. Загрози також включають вразливості ланцюгів постачання та кіберризики, пов'язані із штучним

інтелектом та геополітичною мотивацією [13]. Масштаб і системність цих загроз унеможливлюють їх подолання виключно силами окремих суб'єктів господарювання, що й зумовлює першочергову роль державних політичних механізмів.

Політичні механізми стають ключовими для протидії загрозам інформаційній безпеці, оскільки вразливості підприємств у гібридній війні вимагають державної координації. Необхідні комплексні політичні рамки, що інтегрують оборонні можливості і регуляторні стандарти. Аналізує Національну стратегію кібербезпеки, створення Кіберзбройних сил у 2025 році та проект кібергігієни, що перетворюють політичні пріоритети на практичні заходи для зміцнення національної кіберстійкості [14]. Відправною точкою для розуміння цих механізмів є стратегічна нормативна база, навколо якої вибудовується вся система захисту інформаційної безпеки підприємств.

Саме на цій стратегічній основі розпочинається детальний розгляд механізмів, через які держава практично втілює свою політику захисту як критичної інфраструктури, так і бізнес-сектору від гібридних загроз.

Стратегічна система кібербезпеки України зазнала значних змін, а Національна стратегія кібербезпеки (2021 — 2025 рр.) стала основоположним документом, у якому наголошується на важливості стримування, кіберстійкості та постійного моніторингу мереж. Ця стратегія передбачає розробку плану кіберзахисту, інтегрованого в національний План оборони, та вимагає виділення щонайменше 5 % бюджетних коштів на цифрову інфраструктуру для заходів з кібербезпеки. Ця система була доповнена створенням у жовтні 2025 року на підставі парламентського законопроекту Кібервійськ, які об'єднують наступальні та оборонні військові кіберпотужності під єдиним командуванням у складі Збройних сил, а також кіберрезерв цивільних ІТ-експертів [14]. Ключові складові цієї стратегічної системи та механізми їх реалізації узагальнено в Таблиці 1.

Нормативно-правова підтримка критичної інформаційної інфраструктури є наріжним каменем стратегії кібербезпеки України, зосередженої на виявленні, визначенні пріоритетів та зміцненні ключових секторів, включаючи енергетику, фінанси, телекомунікації, водопостачання, охорону здоров'я та центри обробки даних. Подібно до міжнародних рамок, таких як «Кіберстратегія для Америки 2026», підхід України наголошує на забезпеченні безпеки ланцюгів постачання та зменшенні залежності від постачальників, пов'язаних із супротивниками, що свідчить про посилення відповідальності приватного сектору. Стратегія просуває базові вимоги до кібербезпеки, що відповідають сучасним архітектурам безпеки, включаючи впровадження моделі "нульової довіри", засоби захисту на основі

штучного інтелекту, підготовку до постквантової криптографії та системи багатофакторної автентифікації, стійкі до фішингу [15].

Таблиця 1. Основні компоненти кібербезпеки та механізми їх реалізації

Основний компонент	Стратегічна мета	Механізм реалізації
Захист критичної інфраструктури	Посилення стійкості ключових секторів до гібридних загроз	Обов'язкове виділення 5% бюджету на кібербезпеку
Базові вимоги безпеки	Стандартизація захисту підприємств	Архітектури нульової довіри (Zero Trust) та системи на основі ШІ
Оцінка ризиків, орієнтована на загрози	Безперервна оцінка загроз	Галузеві CERT-центри та центри моніторингу
Інтеграція приватного сектору	Координація взаємодії між державою та бізнесом	Законодавчі рамки та державно-приватні партнерства

Орієнтовані на ризики оцінки є важливою складовою стратегічної структури, що забезпечує постійний аналіз загроз та вразливостей, дозволяючи державі та приватним суб'єктам адаптуватися до постійно мінливого характеру кібератак. Цей підхід визнає, що в умовах активної гібридної війни попередження кібератак неможливе, тому акцент робиться на швидкому виявленні, реагуванні та відновленні операційної діяльності [16]. Постійний моніторинг загроз, у свою чергу, формує інформаційну базу для залучення приватного сектору до спільних оборонних зусиль через відповідні законодавчі механізми.

Законодавчі рамки для залучення приватного сектору перетворюють політичні пріоритети на практичні заходи безпеки за допомогою обов'язкових вимог до звітування про інциденти, обміну інформацією про загрози та дотримання мінімальних стандартів кібергігієни. Ці механізми не вводяться як карна санкція, а як виважена необхідність для коеволюції державних і приватних кіберспроможностей, що забезпечують захист економіки навіть в умовах активної гібридної загрози [17]. На основі цієї стратегічної нормативної бази вибудовується складна інституційна архітектура, призначена для координації дій різних органів влади та забезпечення системної взаємодії між державним і приватним секторами у сфері кібербезпеки.

РНБО є головним координаційним органом України з питань національної безпеки та оборони, який наглядає за ініціативами у сфері кібербезпеки через інституційні механізми. Вона контролює виконавчі органи та

координує діяльність НКЦК. Б. Основні керівники включають Олександра Литвиненка, Рустема Умерова та Василя Малюка, що забезпечує взаємодію між міністерствами та службами для єдиної політики реагування на загрози. [18]. Поруч із РНБО функціонують спеціалізовані виконавчі органи, між якими розподілено конкретні оперативні та нормативні повноваження в системі кіберзахисту.

Державна служба спеціальних комунікацій та захисту інформації (ДССКЗІ) діє як ключовий виконавчий орган у цій системі, встановлює нормативні рамки для кібербезпеки та координує роботу з Міністерством цифрової трансформації. Служба безпеки України (СБУ) надає розвідувальні можливості, тоді як Міністерство закордонних справ займається дипломатичними аспектами. Відомства співпрацюють через НККК для управління інцидентами і протидії кіберзагрозам [19]. Взаємодія між цими відомствами реалізується через чітко вибудувану модель міжвідомчої координації, що охоплює всі рівні управління — від вироблення національної політики до безпосереднього реагування на кіберінциденти на місцях.

Модель міжвідомчої координації забезпечує узгоджені дії через структурований підхід, спираючись на міжнародні практики та координуючи національну політику. Вона передбачає спільну відповідальність державних органів, приватного сектору та громадянського суспільства у зміцненні кібербезпеки. Перший, хто виявляє кіберінцидент, швидко інформує інших, що забезпечує скоординоване реагування. Мережі CERT надають технічні можливості для виявлення та відновлення у секторах економіки, що підкреслює основи для розбудови кіберпотенціалу.

Інституційна архітектура в Україні створює основи для реалізації ініціатив, що посилюють кіберстійкість державних структур і корпоративного сектора. Оперативні програми з кібербезпеки фокусуються на розвитку потенціалу відповідно до стандартів Є. С. Національна стратегія кібергігієни, запланована на листопад 2025 року, містить вимоги до навчання та сертифікації, акцентуючи на основах кібергігієни. Стратегія забезпечує координацію між ключовими установами для охоплення урядових і критичних інфраструктурних секторів [17]. Реалізація цих вимог неможлива без налагоджених каналів обміну інформацією між усіма учасниками системи кіберзахисту, що зумовлює особливу роль спеціалізованих інформаційних платформ.

Платформи для обміну інформацією є важливими механізмами координації розвідданих про загрози і оборонних заходів між державною і приватною сферами. Вони сприяють добровільному обміну кіберзагрозами за моделями, подібними до Закону про обмін інформацією з питань кібербезпеки, з механізмами аудиту і моніторингу. Співпраця між державними та приватними структурами включає ІТ-компанії, волонтерські групи

та організації громадянського суспільства, вирішуючи виклики, пов'язані зі штучним інтелектом і новими векторами атак. Регулярні навчання та симуляції дозволяють перевірити готовність до кібератак, включаючи різні сценарії загроз. Триетапний підхід до навчання формує колективну стійкість і допомагає виявляти прогалини у реагуванні на інциденти. І міжнародне співробітництво значно підвищує кіберстійкість через доступ до новітніх технологій і ресурсів. Внутрішній потенціал кіберстійкості, сформований через такі навчання та програми розбудови потенціалу, суттєво підсилюється завдяки розгалуженій мережі міжнародного співробітництва, яка відкриває доступ до технологій, фінансування та розвідувальних даних, недосяжних у межах однієї країни. Цей міжнародний вимір є критичним для забезпечення довгострокової кіберстійкості українського бізнес-сектору.

Україна розробила комплексні механізми міжнародного співробітництва, які суттєво посилюють інформаційну безпеку підприємств завдяки структурованим партнерським відносинам із структурами НАТО, ЄС, США та Великої Британії. «Талліннський механізм», започаткований у 2023 році 13 країнами, координує виділення 241,7 млн євро на підтримку коротко-, середньо- та довгострокових ініціатив із розбудови кіберпотенціалу, зокрема обмін інформацією про загрози, спільні навчання та захист критичної інфраструктури. Ці партнерства надають українським підприємствам доступ до передових ресурсів у сфері кібербезпеки, зокрема до Резерву кібербезпеки ЄС, а також сприяють гармонізації з такими стандартами ЄС, як NIS2 та DORA, що підвищують стійкість приватного сектору до російської кіберагресії [20]. Декларативні партнерські зобов'язання набувають конкретного практичного виміру через цільові механізми технічної допомоги та грантового фінансування, безпосередньо спрямовані на підприємства і галузеві організації.

Механізми технічної допомоги та грантового фінансування є практичним втіленням цих міжнародних політичних партнерств у сфері підтримки українських підприємств. У лютому 2026 року Нідерланди запустили Фонд кібербезпеки NL-UA, який надає гранти на суму 2,5 млн євро (до 250 000 євро на кожен проект) для нідерландсько-українських консорціумів з кібербезпеки з метою розробки інноваційних рішень у таких сферах, як SOC-as-a-Service, безпека хмарних технологій, управління ідентифікацією та цифрова криміналістика. Аналогічно, естонська організація ESTDEV підтримує рамкові угоди з українськими фірмами до 2030 року, орієнтуючись на державні установи та партнерів з приватного сектору за рахунок донорського фінансування від Sida (12,2 млн євро) та Norad (2,2 млн євро), тоді як ЄС надає до 4 млн євро грантів через Європейський центр компетенції з кібербезпеки для розробки систем кібербезпеки [21].

Поряд із двосторонніми та багатосторонніми грантовими програмами існують і системні виклики міжнародного співробітництва, які визначають межі його ефективності для забезпечення інформаційної безпеки українських підприємств.

Ці міжнародні механізми доповнюють внутрішні зусилля, надаючи можливості, яких окремі країни не можуть забезпечити самостійно, хоча залишаються виклики щодо надійності та стратегічної автономії. Хоча партнерство з НАТО, ЄС та Великою Британією зміцнилося завдяки таким механізмам, як SCEPVA, для координації наступальних кібероперацій, тимчасове призупинення розвідувальної підтримки з боку США на початку 2025 року висвітлило вразливість України, пов'язану з її залежністю від американських ресурсів, оскільки США історично забезпечують 75 — 80 % розвідувальних даних альянсу «П'ять очей». Цей досвід зміцнив модель стійкості України, яка наголошує на прагматичній співпраці, заснованій на довірі, через багатосторонні партнерства, співпрацю між державним і приватним секторами та принцип «нічого про Україну без України», щоб забезпечити довгостроковий цифровий суверенітет, водночас протидіючи постійним гібридним загрозам проти корпоративного сектору [22].

Висновки

Проведене дослідження дозволяє сформулювати узагальнені *висновки* щодо стану та перспектив інформаційної безпеки підприємств України в умовах гібридної війни.

Гібридна агресія Росії сформувала принципово новий ландшафт кіберзагроз для корпоративного сектору, що виходить за межі традиційних моделей захисту. Масований характер атак — понад тисячу задокументованих інцидентів лише у 2024 році — свідчить про перетворення кіберпростору на повноцінний театр воєнних дій, де бізнес-структури є цілеспрямованими об'єктами ураження. Каскадний ефект атак на критичну інфраструктуру безпосередньо дестабілізує операційне середовище підприємств, що вимагає переосмислення самої концепції корпоративної кіберстійкості.

Національна стратегія кібербезпеки (2021 — 2025) заклала інституційне підґрунтя для багаторівневої системи захисту, що охоплює стратегічний, оперативний та інституційний рівні. Ефективність цієї системи безпосередньо корелює з якістю міжвідомчої координації між РНБО, ДССКЗІ, СБУ та Міністерством цифрової трансформації. Досвід 2022 — 2025 років підтверджує, що кіберстійкість підприємств є функцією не лише їхньої власної захищеності, а й загальнонаціональної архітектури управління інцидентами.

Міжнародне партнерство — Талліннський механізм, Резерв кібербезпеки ЄС, Фонд NL-UA — є незамінним компонентом системи захисту, однак тимчасове призупинення американської розвідувальної підтримки на початку 2025 року виявило реальний ризик стратегічної залежності. Це актуалізує принцип «нічого про Україну без України» та необхідність диверсифікації партнерств задля забезпечення довгострокового цифрового суверенітету в умовах тривалої збройної агресії.

Список посилань

1. Пашковський В. Ф. Ідентифікація політико-правових механізмів інформаційної безпеки держави в умовах гібридної війни. Політичне життя. 2025. № 3. С. 114-120. DOI: https://doi.org/10.31558/2519-2949.2025.3.15
2. Хмиров І. М. Механізми державного регулювання інформаційної політики в умовах гібридних загроз як ключовий елемент державного суверенітету. 2024. № 2. С. 45-52. DOI: https://doi.org/10.52363/2414-5866-2024-2-17
3. Ніценко В., Остапенко Р. Моделювання бізнес-процесів підприємства. Бізнес-моделі для сталого розвитку: виклики та цифрова трансформація: тези доповідей Міжнар. наук.-практ. конф. (15-16 лютого 2024 р., м. Харків, Україна). Харків. ХНУ ім. В. Н. Каразіна, 2024. С. 144-146.
4. Ніценко В. С., Остапенко Р. М. Сучасна трансформація маркетингових інструментів в умовах цифрової економіки. Маркетинг XXI століття: виклики змін: матеріали Міжнародної науково-практичної конференції, присвяченої 25-річчю заснування кафедри маркетингу і комерційної діяльності ХДУХТ, 8 — 10 жовтня 2020р. / редкол.: О. І. Черевко [та ін.]. — Х.: ХДУХТ, 2020. С. 86-88.
5. Ніценко В. С., Соломчук Л. М. Економічна безпека як стан ефективності використання корпоративних ресурсів підприємства. Цілі сталого розвитку третього тисячоліття: виклики для університетів наук про життя: Міжнародна науково-практична конференція, м. Київ, Україна, 23 — 25 травня 2018 року: матеріали конференції; Національний університет біоресурсів і природокористування України. К.: ТОВ «ПРІНТЕКО», 2018. Т. 1. С. 192-193.
6. Kachkovska L., Maleonchuk H., Ziniuk D. Information Influence in the Conditions of Hybrid Warfare. Науковий вісник Волинського національного університету імені Лесі Українки. Серія: Міжнародні відносини. 2022. № 3. С. 87 — 102. DOI: https://doi.org/10.29038/2524-2679-2022-03-87-102

7. Редзюк В., Редзюк Н. Формування державної інформаційної політики України в умовах гібридної війни. 2024. Вип. 10. С. 93 — 101. DOI: https://doi.org/10.31470/2786-6246-2024-10-93-101
8. Nofenko A. Russia's Hybrid War Against Ukraine: Information Attack and Mechanisms of Countering. Науковий вісник Волинського національного університету імені Лесі Українки. Серія: Міжнародні відносини. 2019. № 2. С. 68 — 77. DOI: https://doi.org/10.29038/2524-2679-2019-02-68-77
9. Радченко О. В., Чмир Я. І. Гібридна війна як ключова загроза національному суверенітету України. 2021. № 3. С. 45-52. DOI: https://doi.org/10.32851/tnv-pub.2021.3.14
10. Хмиров І., Хмирова А., Бирняк М. Методологічні засади формування та реалізації державної інформаційної політики в умовах гібридних загроз. 2025. Вип. 8. С. 79-88. DOI: https://doi.org/10.32620/pls.2025.8.79
11. Пронін А. Інформаційна безпека як відповідь на гібридні виклики в умовах нової геополітичної динаміки. 2025. С. 22-35. DOI: https://doi.org/10.36074/logos-09.05.2025.041
12. Лелет Я. Механізми та форми забезпечення інформаційної безпеки в умовах кризи. 2025. № 21. С. 1-8. DOI: https://doi.org/10.32782/2312-1815/2025-21-23
13. State Service of Special Communications and Information Protection of Ukraine. Annual Report on Cyber Incidents in Ukraine 2024. Kyiv, 2025. URL: https://scpc.gov.ua/api/files/4560c0ba-c6c0-4935-b48d-0232dd659df3
14. Стратегія кібербезпеки України: затв. Указом Президента України від 26 серп. 2021 р. № 447 / Державна служба спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini
15. Закон України «Про критичну інфраструктуру» від 16 листоп. 2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
16. Постанова Кабінету Міністрів України від 26 листоп. 2025 р. № 1533 «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» (Національний план реагування на кіберінциденти, кібератаки та кіберзагрози). URL: https://cybersec.net.ua/normatyvni-dokumenty/943-deiaki-pytannia-reahuvannia-na-kiberintsydenty-kiberataky-ta-kiberzahrozy.html
17. Міністерство цифрової трансформації України. Мінцифри представило проект Національної

стратегії кіберігієни. 2025. URL: https://www.kmu.gov.ua/news/mintsyfry-predstavyly-proekt-natsionalnoi-stratehii-kiberhihiieny

18. Рада національної безпеки і оборони України. Національний координаційний центр кібербезпеки: діяльність та міжнародне співробітництво. URL: https://www.rnbo.gov.ua/en/Diialnist/7477.html
19. Davydiuk A., Potii O. National Cybersecurity Governance: Ukraine. Tallinn: NATO CCDCOE, 2024. 52 p. URL: https://ccdcoe.org/uploads/2024/08/National-Cybersecurity-Governance_Ukraine_Davydiuk_Potii_2024.pdf
20. Tallinn Mechanism: Two Years of Coordinated International Support for Ukraine's Cyber Resilience. Digital State. 2025. URL: https://digitalstate.gov.ua/en/news/it-outsourcing/tallinn-mechanism-two-years-of-coordinated-international-support-for-ukraines-cyber-resilience
21. Netherlands Launches €2.5 Million Cybersecurity Fund to Support Ukraine. NL-UA Cybersecurity Fund. 2026. URL: https://uatv.ua/en/netherlands-launches-e2-5-million-cybersecurity-fund-to-support-ukraine
22. Hardening Norms and Networks: Europe's Cyber Defence Posture after Ukraine. Intereconomics. 2024. Vol. 59, № 4. URL: https://www.intereconomics.eu/contents/year/2024/number/4/article/hardening-norms-and-networks-europe-s-cyber-defence-posture.html

References

1. Pashkovskyi, V.F. (2025). Identyfikatsiia polityko-pravovykh mekhanizmiv informatsiinoi bezpeky derzhavy v umovakh hibrydnoi viiny [Identification of political and legal mechanisms of information security of the state in the conditions of hybrid war]. Informatsiina bezpeka liudyny, suspilstva, derzhavy, 3, 8-21. [in Ukrainian].
2. Khmyrov, I.M. (2024). Mekhanizmy derzhavnoho rehuliuvannia informatsiinoi polityky v umovakh hibrydnykh zahroz yak kliuchovyi element derzhavnoho suverenitetu [Mechanisms of state regulation of information policy in the context of hybrid threats as a key element of state sovereignty], 2, 45-52. [in Ukrainian].
3. Nitsenko, V. & Ostapenko, R. (2024). Modeliuvannia biznes-protsesiv pidpryiemstva [Modeling of business processes of the enterprise]. Biznes-modeli dlia staloho rozvytku: vyklyky ta tsyfrova transformatsiia, 144-146. [in Ukrainian].

4. Nitsenko, V.S. & Ostapenko, R. M. (2020). Suchasna transformatsiia marketynhovykh instrumentiv v umovakh tsyfrovoi ekonomiky [Modern transformation of marketing tools in the digital economy]. Marketynh XXI stolittia: vyklyky zmin, 86-88. [in Ukrainian].
5. Nitsenko, V.S., & Solomchuk, L. M. (2018). Ekonomichna bezpeka yak stan efektyvnosti vykorystannia korporatyvnykh resursiv pidpryiemstva [Economic security as a state of efficiency of corporate resources usage]. Tsili staloho rozvytku tretoho tysiacholittia, 1, 192-193. [in Ukrainian].
6. Kachkovska, L., Maleonchuk, H., & Ziniuk, D. (2022). Information Influence in the Conditions of Hybrid Warfare. Naukovyi visnyk Volynskoho natsionalnoho universytetu imeni Lesi Ukrainky. Seriia: Mizhnarodni vidnosyny, 3, 87-102.
7. Redziuk, V. & Redziuk, N. (2024). Formuvannia derzhavnoi informatsiinoi polityky Ukrainy v umovakh hibrydnoi viiny [Formation of state information policy of Ukraine in the conditions of hybrid war], 10, 93-101. [in Ukrainian].
8. Nofenko, A. (2019). Russia's Hybrid War Against Ukraine: Information Attack and Mechanisms of Countering. Naukovyi visnyk Volynskoho natsionalnoho universytetu imeni Lesi Ukrainky. Seriia: Mizhnarodni vidnosyny, 2, 68-77.
9. Radchenko, O.V., & Chmyr, Ya.I. (2021). Hibrydna viina yak kliuchova zahroza natsionalnomu suverenitetu Ukrainy [Hybrid war as a key threat to the national sovereignty of Ukraine], 3, 45-52. [in Ukrainian].
10. Khmyrov, I., Khmyrova, A., & Byrniak, M. (2025). Metodolohichni zasady formuvannia ta realizatsii derzhavnoi informatsiinoi polityky v umovakh hibrydnykh zahroz [Methodological principles of formation and implementation of state information policy in the context of hybrid threats], 8, 79-88. [in Ukrainian].
11. Pronin, A. (2025). Informatsiina bezpeka yak vidpovid na hibrydni vyklyky v umovakh novoi heopolitychnoi dynamiky [Information security as a response to hybrid challenges in the new geopolitical dynamics], 22-35. [in Ukrainian].
12. Lelet, Ya. (2025). Mekhanizmy ta formy zabezpechennia informatsiinoi bezpeky v umovakh kryzy [Mechanisms and forms of ensuring information security in crisis conditions], 21, 1-8. [in Ukrainian].

13. State Service of Special Communications and Information Protection of Ukraine. (2025). Annual Report on Cyber Incidents in Ukraine 2024. Kyiv.
14. Stratehiia kiberbezpeky Ukrainy [Cybersecurity Strategy of Ukraine]. (2021). URL: https://cip.gov.ua/ua/news/strategiya-kiberbezpeki-ukrayini [in Ukrainian].
15. Zakon Ukrainy «Pro krytychnu infrastrukturu» [Law of Ukraine «On Critical Infrastructure»]. (2021). URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text [in Ukrainian].
16. Postanova Kabinetu Ministriv Ukrainy «Deiaki pytannia reahuvannia na kiberintsydenty, kiberataky ta kiberzahrozy» [Resolution of the Cabinet of Ministers of Ukraine «Some issues of response to cyber incidents, cyber attacks and cyber threats»]. (2025). URL: https://cybersec.net.ua/normatyvni-dokumenty/943-deiaki-pytannia-reahuvannia-na-kiberintsydenty-kiberataky-ta-kiberzahrozy.html [in Ukrainian].
17. Ministry of Digital Transformation of Ukraine. (2025). Mintsyfry predstavylo proekt Natsionalnoi stratehii kiberhihiieny [Ministry of Digital Transformation presented the draft National Cybersecurity Strategy]. URL: https://www.kmu.gov.ua/news/mintsyfry-predstavyly-proekt-natsionalnoi-stratehii-kiberhihiieny [in Ukrainian].
18. National Security and Defense Council of Ukraine. (n.d.). Natsionalnyi koordynatsiinyi tsentr kiberbezpeky: diialnist ta mizhnarodne spivrobitnytstvo [National Cybersecurity Coordination Center: activities and international cooperation]. URL: https://www.rnbo.gov.ua/en/Diialnist/7477.html [in Ukrainian].
19. Davydiuk, A. & Potii, O. (2024). National Cybersecurity Governance: Ukraine. Tallinn: NATO CCDCOE.
20. Tallinn Mechanism: Two Years of Coordinated International Support for Ukraine's Cyber Resilience. (2025). Digital State.
21. Netherlands Launches €2.5 Million Cybersecurity Fund to Support Ukraine. (2026). NL-UA Cybersecurity Fund.
22. Hardening Norms and Networks: Europe's Cyber Defence Posture after Ukraine. (2024). Intereconomics, 59(4).

UDC 323:004.056:658 DOI 10.17721/2415-881X.2026.100.1.342–358

Ivan Fomin
Postgraduate Student of the Department of Political Science, Sociology and Cultural Studies, Faculty of Social and Humanitarian Sciences and Social Technologies, H. S. Skovoroda Kharkiv National Pedagogical University (Kharkiv, Ukraine)
https://orcid.org/0009-0007-7593-9134
e-mail: bezpeka.khladik@gmail.com

POLITICAL MECHANISMS FOR ENSURING INFORMATION SECURITY IN ENTERPRISES IN THE CONTEXT OF HYBRID WARFARE

Abstract

This article provides a comprehensive analysis of the political mechanisms and strategic frameworks for ensuring the information security of Ukrainian enterprises in the context of hybrid warfare. The relevance of the study stems from the transformation of the threat environment resulting from massive Russian cyber aggression, which is shaping a fundamentally new risk landscape for the corporate sector that goes beyond traditional cybersecurity models. In this context, corporate information security is viewed not as a purely technical problem, but as an integral component of national cyber resilience and the state's digital sovereignty.

Particular attention is paid to the analysis of Ukraine's National Cybersecurity Strategy (2021 — 2025) as a foundational document that lays the institutional groundwork for a multi-level protection system. It is demonstrated that the effectiveness of this system directly correlates with the quality of interagency coordination between the National Security and Defense Council, the State Service for Cybersecurity and Information Protection, the Security Service of Ukraine, and the Ministry of Digital Transformation, while the cyber resilience of enterprises is a function not only of their own security but also of the nationwide incident management architecture. The mechanisms for engaging the private sector through legislative frameworks, public-private partnerships, and industry CERT centers have been examined.

The role of international cooperation-the Tallinn Mechanism, the EU Cybersecurity Reserve, and the NL-UA Cybersecurity Fund-as an indispensable component of the defense system has been analyzed. At the same time, it has been demonstrated that the temporary suspension of U.S. intelligence support in early 2025 revealed a real risk of strategic dependence and highlighted the need to diversify partnerships in accordance with the principle of "nothing about Ukraine without Ukraine." The concept of multi-level resilience has been introduced, implemented through the interaction of government regulators, business, and civil society organizations.

In conclusion, the thesis is substantiated that ensuring the information security of enterprises in the context of hybrid warfare is impossible without integrating corporate protection into a unified nationwide cyber resilience system. The limitations of purely technical approaches to cyber defense in conditions of geopolitical instability are highlighted, and the importance of institutional coordination, international partnerships, and the implementation of basic security requirements (zero-trust architecture, multi-factor authentication, post-quantum cryptography) to ensure the state's long-term digital sovereignty in the context of prolonged armed aggression.

Keywords: information security; corporate cybersecurity; hybrid warfare; critical information infrastructure; public-private partnership; cyber resilience; digital sovereignty.

Надійшла до редакції/ Received: 23.01.2026

Прорецензовано/ Revised: 11.02.2026

Прийнято до друку/ Accepted: 27.02.2026