УДК 004.056
DOI: https://doi.org/10.24144/2307-3322.2026.94.2.57

ПРАВОВІ МЕХАНІЗМИ ЗАБЕЗПЕЧЕННЯ КІБЕРСТІЙКОСТІ СЕКТОРУ БЕЗПЕКИ Й ОБОРОНИ В УМОВАХ ВОЄННОГО СТАНУ

Пащенко Є.М.,
доктор філософії в галузі права (PhD),
старший викладач кафедри
Військово-юридичного інституту
Національного юридичного університету
імені Ярослава Мудрого
ORCID: 0000-0002-7178-0601

Пащенко Є.М. Принцип гуманізму, як основоположний принцип побудови сучасної правової держави.

У статті комплексно досліджуються правові механізми, що гарантують кіберстійкість сектору безпеки й оборони (СБО) України в реаліях воєнного стану, запровадженого через повномасштабну збройну агресію рф. Оскільки сучасні збройні конфлікти стрімко трансформуються у гібридні, кіберпростір остаточно перетворився на самостійне операційне середовище. Сьогодні атаки на критичну інфраструктуру та інформаційні ресурси Збройних Сил є невід'ємною складовою російської гібридної агресії. За таких умов дієва та гнучка правова база стає критично необхідною для збереження обороноздатності країни та стабільної роботи СБО.

У роботі здійснено системний аналіз чинного законодавства у сфері кібербезпеки. Зокрема, розглянуто закони України «Про основні засади забезпечення кібербезпеки України», «Про правовий режим воєнного стану», «Про критичну інфраструктуру», Стратегію кібербезпеки України, а також відповідну підзаконну базу Міноборони та Генерального штабу ЗСУ. Значний акцент зроблено на тому, як вітчизняні норми еволюціонують від класичного розуміння кібербезпеки до парадигми «кіберстійкості» в умовах відкритої війни, а також на процесі впровадження євроатлантичних практик і Директиви ЄС NIS2.

Також проаналізовано систему державних суб'єктів забезпечення кіберстійкості (ДССЗЗІ, СБУ, СЗР та Командування з кібероперацій ЗСУ) і виявлено низку системних колізій у розподілі їх компетенцій. З'ясовано, що чинне законодавство досі не має цілісного механізму для урегулювання воєнних кібероперацій, оминає питання правового статусу ІТ-волонтерів і не містить процедури перевірки дій ЗСУ в кіберпросторі на відповідність міжнародному гуманітарному праву (з огляду на стандарти Талліннського посібника 3.0 2023 року). Виокремлено головні юридичні прогалини: термінологічну невизначеність, слабку інституалізацію Кіберсил ЗСУ в контексті наступальних операцій, а також неврегульованість залучення приватного сектору до захисту інфраструктури.

Окремо розглянуто екстраординарні кроки, до яких держава вдалася під час війни – наприклад, перенесення державних реєстрів у закордонні хмарні середовища та залучення хактивістів до відновлення інфосистем. Серед запропонованих шляхів удосконалення законодавства: декриміналізація дій українських кіберволонтерів, ухвалення спеціального закону «Про Кіберсили Збройних Сил України», розробка єдиного Кіберкодексу України та чітке розмежування захисних, розвідувальних і наступальних операцій (із закріпленням рівня авторизації та парламентського контролю для кожної).

Спираючись на порівняльно-правовий аналіз, у статті обґрунтовано потребу в масштабній інституційній реформі – зокрема, створенні міжвідомчої Ради кібербезпеки та оборони. Отримані результати можуть бути корисними для законопроєктної роботи профільних комітетів Верховної Ради, а також у науково-дослідній сфері публічного та інформаційного права.

Ключові слова: кіберстійкість, кібербезпека, сектор безпеки й оборони, воєнний стан, правові механізми, критична інфраструктура, кіберзахист, кібероперації, міжнародне гуманітарне право, НАТО, NIS2, ІТ-армія.

Pashchenko Y.M. Legal mechanisms for ensuring cyber resilience in the security and defense sector under martial law.

This article provides a comprehensive examination of the legal mechanisms that ensure the cyber resilience of Ukraine's security and defense sector (SDS) under the conditions of martial law, which was imposed in response to the Russian Federation's full-scale armed aggression. As modern armed conflicts rapidly transform into hybrid conflicts, cyberspace has definitively become an independent operational environment. Today, attacks on the critical infrastructure and information resources of the Armed Forces are an integral part of Russian hybrid aggression. Under such conditions, an effective and flexible legal framework becomes critically necessary to preserve the country's defense capability and the stable operation of the SDS.

This paper provides a systematic analysis of current cybersecurity legislation. Specifically, it examines the laws of Ukraine "On the Basic Principles of Ensuring Ukraine's Cybersecurity", "On the Legal Regime of Martial Law," "On Critical Infrastructure," the Cybersecurity Strategy of Ukraine, as well as the relevant subordinate legislation of the Ministry of Defense and the General Staff of the Armed Forces of Ukraine. Significant emphasis is placed on how domestic regulations are evolving from a classical understanding of cybersecurity to a "cyber resilience" paradigm in the context of open warfare, as well as on the process of implementing Euro-Atlantic practices and the EU NIS2 Directive.

The study also analyzed the system of state entities responsible for ensuring cyber resilience (the State Service for Cyber Security and Information Protection, the Security Service of Ukraine, the Foreign Intelligence Service, and the Cyber Operations Command of the Armed Forces of Ukraine) and identified a number of systemic conflicts in the distribution of their responsibilities. It was found that current legislation still lacks a comprehensive mechanism for regulating military cyber operations, bypasses the issue of the legal status of IT volunteers, and does not include a procedure for verifying the Armed Forces' actions in cyberspace for compliance with international humanitarian law (in light of the standards of the Tallinn Manual 3.0 2023). The main legal gaps were identified: terminological ambiguity, weak institutionalization of the Armed Forces' Cyber Forces in the context of offensive operations, as well as the lack of regulation regarding the involvement of the private sector in infrastructure protection.

Separately, the paper examines the extraordinary measures the state has taken during the war – for example, the transfer of state registries to foreign cloud environments and the involvement of hacktivists in restoring information systems. Among the proposed ways to improve legislation are: decriminalizing the actions of Ukrainian cyber volunteers, adopting a special law "On the Cyber Forces of the Armed Forces of Ukraine," developing a unified Cyber Code of Ukraine, and clearly distinguishing between defensive, intelligence, and offensive operations (with established levels of authorization and parliamentary oversight for each).

Based on a comparative legal analysis, this article substantiates the need for large-scale institutional reform–specifically, the establishment of an interagency Council on Cybersecurity and Defense. The findings may be useful for the legislative work of the relevant committees of the Verkhovna Rada, as well as in the field of research on public and information law.

Key words: cyber resilience, cybersecurity, security and defense sector, martial law, legal mechanisms, critical infrastructure, cyber defense, cyber operations, international humanitarian law, NATO, NIS2, IT army.

Постановка проблеми. Стрімка цифровізація інформаційного простору України та активне впровадження ІТ-систем у секторі безпеки й оборони супроводжуються безпрецедентним зростанням загроз. Шпигунські операції, інформаційні кампанії та постійні спроби впровадити шкідливе ПЗ у державні ресурси стали буденністю. Ця проблема максимально загострилася з початком воєнного стану, коли критичні об'єкти СБО опинилися під безперервним ударом з боку рф. Від здатності витримувати такі атаки залежить обороноздатність країни.

Сучасна модель ведення війн остаточно затвердила кіберпростір як повноцінний, п'ятий операційний домен, який працює на одному рівні із суходолом, морем, повітрям та космосом. Досвід повномасштабного вторгнення показав: цифрові атаки ніколи не відбуваються у вакуумі, вони чітко синхронізовані з кінетичними діями. Так, «покладення» енергосистем передує ракетним ударам, компрометація мереж зв'язку йде пліч-о-пліч із наземними наступами, а російські ІПСО в мережі лише посилюють тиск на суспільство та військовослужбовців на фронті. Ця синхроні-

зація доводить, що кіберстійкість СБО перестала бути лише технічним завданням – сьогодні це фундаментальна державна проблема.

І хоча нормативно-правових актів у цій сфері чимало, їх ефективність в умовах війни виявилася обмеженою. Класична концепція «кібербезпеки», яка робила ставку переважно на превентивний захист і побудову «глухого» периметра, не витримує реалій активного конфлікту. Серед найгостріших проблем: розмиті повноваження державних органів, брак алгоритмів швидкого реагування, прогалини в кримінальному праві та слабка інтеграція з міжнародними стандартами. Крім того, українські закони досі не сформували спеціального правового режиму для кіберпростору на період воєнного стану, не відрізняють цивільний захист від воєнних операцій, не регулюють наступальні дії у вигляді гібридних форм ведення війни в мережі і юридично «не бачать» кіберволонтерів. Відповідно, державі потрібен перехід від класичного захисту до «кіберстійкості». Йдеться про здатність електронних мереж витримувати деструктивні впливи, адаптуватися до них і безперервно виконувати свої функції навіть за часткового ураження. І це серйозний юридичний виклик, адже більшість наявних норм видані для умов мирного часу і не враховують комплекс дій у прийнятті інформаційно-безпекових рішень для забезпечення оборони.

Окрема складність – інституційна роздробленість. Відповідальність за захист в інформаційній сфері зараз розділена між ДССЗЗІ, СБУ, СЗР, НПУ та ЗСУ. При цьому їх компетенції на рівні закону розмежовані не чітко. Крім цього, повільне удосконалення нормативної бази України у відповідності до норм міжнародного права зазначених у міжнародних виданнях (наприклад: Талліннському посібнику 3.0) та директиві ЄС NIS2 суттєво ускладнює запровадження процедур виявлення і забезпечення безпеки кібероперацій.

Метою дослідження є комплексне вивчення правових механізмів забезпечення кіберстійкості сектору безпеки й оборони України під час воєнного стану, а також виявлення системних прогалин та юридичних колізій у чинному законодавстві. Дослідження спрямоване на розробку теоретико-прикладних рекомендацій для вдосконалення нормативної бази з урахуванням норм міжнародного гуманітарного права, стандартів НАТО та директив ЄС.

Для досягнення цієї мети слід приділити увагу дослідженню та аналізу наступних питань: аналіз нормативно-правової бази у сфері кібербезпеки СБО та оцінити її життєздатність під час війни; порівняльно-правовий аналіз українських норм щодо наявності пропонованих вимог Директив ЄС NIS2 і стандартів НАТО для визначення пріоритетів їх гармонізації; дослідити статус нових суб'єктів (IT Army of Ukraine, кіберволонтери) в рамках пропозицій створення концептуальних підходів до їх легалізації.

Аналіз останніх досліджень і публікацій. Питання правового забезпечення кіберстійкості оборонного сектору очікувано привертає значну увагу наукової спільноти, особливо на тлі гібридних викликів. Проте специфіка цього забезпечення саме в екстремальних умовах відкритого воєнного конфлікту залишається розкритою лише фрагментарно.

Серед вітчизняного наукового середовища щодо питань дослідження інформаційної та кібербезпеки доцільно виділити таких науковців, як: Б.А. Кормич (сформував концептуальний апарат адміністративно-правового регулювання інфосфери) та О.Д. Довгань (досліджував суб'єкти кіберзахисту та правове регулювання реагування на інциденти). Однак фундаментальні праці здебільшого мають теоретичний характер і писалися переважно з огляду на реалії мирного часу.

На міжнародному рівні величезний внесок у доктрину регулювання кібероперацій зробили М. Шмітт, Г. Корнер та Т. Рід. Зокрема, матеріали «Талліннського посібника» (Tallinn Manual) [14] та роботи М. Шмітта детально пояснюють, як норми міжнародного гуманітарного права застосовуються до цифрового середовища, за яких умов кібератаку можна вважати збройним нападом та як визначати статус таких як «IT Army of Ukraine». Роботи Г. Корнера зосереджені на розмежуванні кібершпигунства та наступальних операцій. Емпіричну базу про кібератаки та ефективність правового реагування на них дають аналітичні звіти ENISA, CCDCOE, Microsoft Digital Defense Report та Mandiant Threat Intelligence.

Слід визнати, що більшість наукових праць опиралася на досвід гібридних конфліктів низької інтенсивності. Натомість екстраординарне правове регулювання під час повномасштабної війни залишається «білою плямою». Досі бракує ґрунтовного аналізу таких рішень, як транскордонна міграція суверенних даних, застосування тактики hack back або інституалізація Кіберсил ЗСУ.

Стан опрацювання проблематики. Об'єктом дослідження є суспільні відносини у сфері забезпечення кіберстійкості СБО України в умовах воєнного стану, а предметом – правові механіз-

ми регулювання цих відносин (законодавча база, інституційна архітектура, міжнародні зобов'язання).

Виклад основного матеріалу. Правове забезпечення кіберстійкості сектору безпеки й оборони (СБО) України ґрунтується на багаторівневій нормативній системі, яка охоплює конституційний, законодавчий, підзаконний та міжнародно-правовий рівні. Основу механізму складають Конституція України, закони «Про основи національної безпеки України», «Про оборону України», «Про кібербезпеку України», «Про правовий режим воєнного стану» та підзаконні акти, а також стратегічні документи, зокрема Стратегія кібербезпеки України [1, 2, 3, 4, 5]. Ці нормативні документи визначають правову основу для створення та функціонування систем протидії кібератакам, регламентують відповідальність за порушення та формують порядок взаємодії державних органів, військових формувань і приватного сектору.

З початком повномасштабного вторгнення російської федерації концептуальні підходи до кіберзахисту зазнали кардинальних змін. Традиційна модель, що базувалася на розбудові ешелонованих систем захисту, в умовах інтенсивних і безперервних атак виявилася вразливою. Ключовим завданням держави стало забезпечення кіберстійкості – здатності критичної інформаційної інфраструктури та систем СБО адаптуватися до загроз, витримувати удари та швидко відновлювати свою функціональність. Це передбачає не лише оборонний захист, а й здатність до превентивних заходів і оперативного реагування із залученням міжнародного партнерства [4, 10, 11].

На конституційному рівні правовою основою кіберзахисту застосовуються статті 17 і 92 Конституції України, які закріплюють обов'язок держави щодо захисту суверенітету та встановлюють законодавчий характер регулювання питань національної безпеки й оборони. Водночас Конституція не містить згадки про кіберпростір як об'єкт державного захисту, що ускладнює формування цілісної правової доктрини [1]. Базовим законодавчим актом у сфері кібербезпеки є Закон України «Про основні засади забезпечення кібербезпеки України», який встановлює понятєвий апарат галузі та систему реагування на кіберінциденти, проте не враховує реалії воєнного стану [4]. Закон «Про правовий режим воєнного стану» надає військовому командуванню широкі повноваження щодо обмеження діяльності в інформаційній сфері, але його положення не адаптовані під особливості кібероперацій [5].

Стратегія кібербезпеки України визначає стратегічні цілі та пріоритети розвитку системи, орієнтуючи країну на євроатлантичну інтеграцію та розмежування цивільного й військового кіберзахисту, проте конкретні правові механізми реалізації цих цілей залишаються чітко не сформованими. В умовах війни значущість набувають окремі правові інструменти, наприклад легалізація «хмарної міграції» державних даних для захисту від руйнувань критичної інфраструктури. [10, 12, 13]

Інституційна архітектура кіберстійкості характеризується множинністю суб'єктів без чіткої ієрархії та законодавчо визначених меж компетенції. Основні елементи забезпечення державного рівня включають: Державну службу спеціального зв'язку та захисту інформації (Держспецзв'язок), яка координує реагування на кібератаки та підтримує CERT-UA; Службу безпеки України (СБУ), що здійснює контррозвідувальну та оперативно-розшукову діяльність у кіберпросторі; Службу зовнішньої розвідки (СЗР), яка займається кіберрозвідкою поза межами держави; Війська зв'язку та кібербезпеки Збройних Сил України, яке формує воєнний кіберпотенціал та здійснює активну кібероборону.

Наявність дублювання повноважень, відсутність чітких правових меж і координаційних процедур призводить до правових прогалин і ускладнює інтеграцію до кіберструктур НАТО. [7, 8, 9].

Координаційний центр – Рада національної безпеки і оборони України (РНБО) – забезпечує стратегічне керівництво, однак без функції оперативної міжвідомчої координації, аналогічної Cyber Operations Center в країнах НАТО. Для ефективної кіберстійкості важлива взаємодія державного та приватного секторів, зокрема ІТ-компаній і добровольчих об'єднань («ІТ-армія України»), що піднімає питання відповідальності за протидію кібератак.

Найбільш критичною прогалиною є відсутність правового регулювання кібероперацій ЗСУ. Законодавство не визначає перелік уповноважених дій, рівень авторизації для операцій, правові обмеження щодо вибору цілей та взаємодію з СБУ і СЗР. Це створює ризики для координації оборонних і наступальних дій у кіберпросторі, зокрема щодо застосування активної кібероборони.

У воєнний час правовий механізм трансформувався: військове командування отримало право управляти підприємствами та телекомунікаційними ресурсами, блокувати ворожі сайти, а на рівні державних систем інформацію розміщувати на хмарних сервісах іноземних партнерів. Це

забезпечує безперервність державного управління та захист унікальних баз даних, включно з реєстрами військовозобов'язаних та логістичними системами.

Превентивні заходи включають визначення правових вимог до проектування та експлуатації систем, застосування антивірусного захисту, шифрування критичної інформації, систем виявлення вторгнень та регулярне навчання персоналу.

Оперативні заходи передбачають швидке реагування на інциденти: виявлення джерела загрози, локалізацію наслідків та відновлення працездатності систем у режимі реального часу. Законодавство визначає повноваження органів щодо координації дій з іншими державними та приватними структурами. [6].

Відновлювальний аспект включає відновлення даних, цифрові експертизи, створення резервних копій та систем моніторингу для забезпечення неперервності функціонування державних органів і військових формувань

Україна активно імплементує міжнародні стандарти НАТО та ЄС у сфері кібербезпеки, зокрема NIS2 Directive. Це забезпечує оцінку ризиків, планування реагування, навчання персоналу та координацію з союзниками. Встановлення правових вимог до кіберстійкості всього ланцюга постачання та контроль приватних підрядників є важливим елементом інтеграції та підвищення ефективності захисту СБО. [12]

Незважаючи на досягнення, система правового забезпечення кіберстійкості має низку проблем: законодавчі прогалини щодо кримінальної відповідальності за кібератаки; невизначеність правового статусу суб'єктів кібербезпеки, зокрема волонтерів; відсутність єдиного механізму координації між цивільними і військовими структурами; термінологічні прогалини у визначеннях «кібервійна», «кіберзброя», «кібероперація».

Ці прогалини створюють ризики для ефективного реагування на загрози та мінімізації наслідків кібератак, що підкреслює необхідність прийняття спеціалізованих нормативно-правових актів і розвитку системи моніторингу та контролю.

Висновки. Правове забезпечення кіберстійкості сектору безпеки та оборони України є багаторівневим і комплексним процесом, що охоплює конституційний, законодавчий, підзаконний та міжнародно-правовий рівні. Основу цього механізму формують Конституція України та ключові закони, зокрема «Про національну безпеку України», «Про оборону України», «Про основи забезпечення кібербезпеки» та Закон «Про правовий режим воєнного стану». Проте система кіберзахисту розвивалася ситуативно, під впливом конкретних загроз, що призвело до фрагментарності нормативної бази та окремих суперечностей. Сучасна війна показала, що чинні норми не враховують особливостей ведення кібероперацій у кризових умовах і потребують суттєвого вдосконалення.

З початком агресії росії перед нашою державою постало завдання забезпечити кіберстійкість – здатність критичної інфраструктури та систем сектору безпеки та оборони витримувати кібернетичні удари та швидко відновлювати функціонування. Це потребувало трансформації управлінських процедур, розширення повноважень військового командування та державних органів, легалізації практик хмарної міграції даних і залучення кіберволонтерів. Досвід показав високу гнучкість правового механізму: завдяки оперативним рішенням у межах воєнного стану держава змогла вистояти під системними ударами ворога.

Водночас ефективність кібероборони досягалася часто ситуативно, через рішення «ad hoc» та підзаконні акти. Існуюча нормативно-правова база містить суттєві прогалини: невизначеність термінології («кіберзброя», «кібервійна», «активна кібероборона»), недостатня регламентація взаємодії між суб'єктами кіберзахисту, обмежена інтеграція цивільного та військового кіберзахисту, розпорошеність повноважень та відсутність постійного органу координації.

Для підвищення ефективності кіберстійкості пропонується подолати термінологічний вакуум, врегулювати статус кіберволонтерів, інституалізувати Сил кіберзахисту ЗСУ, імплементувати європейські стандарти NIS2 та розглянути можливість розробки Кібербезпеки вУкраїні.

Дослідження також виявило низку проблем: системна незавершеність нормативної бази, невизначеність статусу Командування з кібероперацій, розпорошеність відповідальності, відсутність механізмів перевірки відповідності кібероперацій міжнародному гуманітарному праву, а також сучасного підходу до стандартів НАТО та ЄС.

Правове забезпечення кіберстійкості перебуває на етапі, коли стихійний розвиток нормативної бази має питання щодо системних підходів та реформ. Унікальний досвід України у реаль-

них умовах кіберпротистояння слугує цінним ресурсом для вдосконалення національної правової системи та формування із залученням партнерів на міжнародному рівні спільної правової доктрини кібероперацій під час збройних конфліктів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конституція України. Документ 254к/96-ВР від 28.06.1996. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#n4537.
2. Про основи національної безпеки України. Документ 964-IV від 19.06.2003. URL: https://zakon.rada.gov.ua/laws/show/964-15#Text.
3. Про оборону України. Документ 1932-XII від 06.12.1991. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text.
4. Про основні засади забезпечення кібербезпеки України. Документ 2163-VIII від 05.10.2017. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
5. Про правовий режим воєнного стану. Документ № 389-VIII від 12.05.2015 URL: https://zakon.rada.gov.ua/laws/show/389-19.
6. Про критичну інфраструктуру. Документ № 1882-IX від 16.11.2021. URL: https://zakon.rada.gov.ua/laws/show/1882-20.
7. Про Державну службу спеціального зв'язку та захисту інформації України. Документ 3475-IV від 23.02.2006. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.
8. Про Службу безпеки України. Документ 2229-XII від 25.03.1992. URL: https://zakon.rada.gov.ua/laws/show/2229-12#Text.
9. Про розвідку. Документ 912-IX від 17.09.2020. URL: https://zakon.rada.gov.ua/laws/show/912-20#Text.
10. Про Стратегію кібербезпеки України. Документ № 447/2021 від 26.08.2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021.
11. Про деякі заходи щодо захисту державних інформаційних ресурсів у межаї передачі даних. Указ Президнта України від 24.09.2001. URL: https://ips.ligazakon.net/document/u891_01?an=274.
12. Directive (EU) 2022/2555 (NIS2 Directive) on measures for a high common level of cybersecurity across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.
13. NATO Cyber Defence Pledge. Brussels: NATO Headquarters, 2023. URL: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/08/cyber-defence-pledge.
14. Tallinn manual 2.0 on the international law applicable to cyber operations / general editor Michael N. Schmitt. Cambridge: Cambridge University Press, 2017. 598 p.

Дата першого надходження рукопису до видання: 01.04.2026
Дата прийняття до друку рукопису після рецензування: 23.04.2026
Дата публікації: 10.05.2026