DOI https://doi.org/10.30525/978-9934-26-686-7-17

ІНСТИТУЦІОНАЛІЗАЦІЯ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ: ПРАВОВИЙ СТАТУС ТА ПОВНОВАЖЕННЯ СУБ'ЄКТІВ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Співак М. В., Дубіна О. М.

ВСТУП

Масштабна російська кіберагресія проти України стала ключовим каталізатором, що не лише виявив критичні вразливості, а й підкреслив екзистенційну необхідність прискореного розвитку національної індустрії продуктів та послуг кібербезпеки. Сучасний стан інформаційного протистояння характеризується безпрецедентною кількістю та складністю атак: Україна стабільно входить до переліку країн світу, що зазнають найбільшого цифрового тиску, поступаючись за інтенсивністю лише США. Лише протягом 2023 року було офіційно зафіксовано 2544 кіберінциденти, що на 16% перевищило показники попереднього року. Ця динаміка свідчить про перехід кіберзагроз у фазу перманентного тиску на державні інституції, оборонно-промисловий комплекс, енергетику та фінансовий сектор. Постійні атаки з боку російських хакерських угруповань, що використовують методи DDoS, розповсюдження програм-вимагачів (Ransomware) та фішингу, змусили український ринок еволюціонувати швидше за світові тренди.

Як наслідок, за останні вісім років обсяг українського ринку кібербезпеки продемонстрував стрімке зростання, збільшившись у чотири рази – з 32 млн доларів у 2016 році до 138 млн доларів у 2024-му. Попри те, що частка України на глобальному ринку поки що становить менше 1%, країна перетворилася на світового трендсеттера та унікальний полігон для R&D-інновацій. Специфіка воєнного стану зумовила домінування сегмента кіберрішень, який займає 57% ринку, випереджаючи глобальний показник, де переважають сервіси. Це пояснюється гострою потребою у впровадженні автоматизованих систем захисту на основі штучного інтелекту, здатних миттєво реагувати на загрози за умов обмеженого людського ресурсу. Прогнози вказують на подальшу інтенсифікацію галузі: очікується, що до 2029 року ринок зросте ще на 50%, досягнувши позначки у 209 млн доларів. Такий розвиток є не просто економічним показником, а стратегічним елементом національної безпеки, оскільки масштаби загроз диктують вимоги до створення повністю автономної та високотехнологічної екосистеми кіберзахисту, здатної протистояти викликам першої у світі повномасштабної кібервійни[1].

[1] Огляд ринку кібербезпеки в Україні : звіт / DataDriven, підкомітет з кібербезпеки EBA, CyberTech комітет Асоціації IT Ukraine за сприяння Аспен Інституту Київ, за підтримки Проєкту USAID. Січень 2025. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf (дата звернення: 10.02.2026).

1. Кібербезпека як багатоаспектне явище: різні підходи до визначення та забезпечення захисту

Світ стрімко змінюється. Нинішнє різко контрастує із вчорашнім. Розвиток нових комунікацій і технологій (зокрема Інтернет) супроводжуються новими дестабілізаційними викликами (сучасні інформаційні війни, кіберзагрози), «полікризами» та «пермакризами» (значна кількість проблем, які виникають одночасно) які почали формуватися ще наприкінці 2010-х років[2]. Однак теоретичним викликом для сучасної науки є не лише проблеми концептуалізацій сучасних трансформацій а й продукування нових типів знання та конструювання нових типів відносин. Позаяк ми живимо за доби глобалізації знань і спільних проблем людства, більша відкритість інформаційного простору потребує захисту. Адже у ньому нашаровуються поєднання національного, соціального, культурного і навіть суто особистого із глобальним, загальнолюдським, універсальним і безпековим. В сучасних умовах проблеми інформаційних відносин актуалізувалися у зв'язку з глобалізацією інформаційних процесів, бурхливим розвитком і пануванням, стало очевидним відокремлення такого явища, як «кібербезпека».

Кібербезпека – це складний і багатогранний процес, що охоплює різні аспекти напрямків, механізмів і методів захисту. Хоча структура кібербезпеки ще не повністю систематизована, її розуміння як комплексної діяльності дозволяє гармонізувати термінологію та глибше проаналізувати суттєві аспекти цієї сфери. Вивчаючи кібербезпеку, необхідно пам'ятати, що вона є невід'ємною частиною інформаційних технологій. У сучасному світі стрімкий розвиток і поширення нових інформаційно-комунікаційних технологій створює умови для глобальної інформаційної революції. Цей процес має безпосередній вплив на всі аспекти діяльності держави, включаючи політичну, економічну, управлінську, фінансову, культурну, наукову та інформаційну сфери. Як слушно зазначає В. Бондаренко людство живе в інформаційному суспільстві. Інформація – є рушійною силою перетворень та розвитку людства, а запорукою його процвітання є людська інтелектуальна творчість. Головним об'єктом, на якому концентрується безпосередній інформаційний деструктивний вплив у межах інформаційної війни, стали громадська думка та свідомість окремої людини. Саме тому духовні, культурні, історичні, етнічні й загальнонаціональні цінності, традиції, надбання держави стають полем кібербитви, адже це той простір, де дуже багато вразливих й чутливих рецепторів суспільства[3].

Нині, особливу увагу приділяється людиноцентричним підходам, збалансованому управлінню ресурсами та розширенні можливостей цифровізації. Цифровізація включає в себе комплексний аналіз та впровадження цифрових технологій у всі аспекти діяльності підприємств. Д. Попова, С. Яременко під кібербезпекою, розуміють систему комплексних заходів, що забезпечують захист

[2] Екзистенційні виклики перед Україною. Демографія. DeepState. 23.09.2023. URL: https://deepstateua.com/iekzistientsialni-vikliki-ukrayini-chastina-i-diemoghrafiia/ (дата звернення: 11.02.2026).

[3] Бондаренко В. Кібербезпека: роль держави у захисті суспільства та окремої особистості у збереженні міжетнічного миру. *Аспекти публічного управління*. 2020. Т. 8, № Спец. вип. 1. С. 18–21. DOI: 10.15421/152031

інформаційних ресурсів, технологій та інфраструктури від загроз будь-якого походження з метою забезпечення стійкості, надійності та безперервного розвитку держави, суспільства та окремих осіб в умовах цифрової трансформації та Індустрії 5.0. На їх думку Індустрію 5.0 не слід сприймати як заміну попередній парадигмі – Індустрії 4.0, а радше як її розвиток та доповнення, яке вносить нові ключові аспекти:

– Людиноцентричний підхід. Індустрія 5.0 підкреслює значення створення безпечного та інклюзивного робочого середовища, де пріоритетом є здоров'я та благополуччя працівників, з метою досягнення не лише високої продуктивності, а й задоволення потреб кожного працівника.

– Стійкість. Здатність швидко адаптуватися до змін є критично важливою для підприємств, які прагнуть залишатися конкурентоспроможними в умовах невизначеності, включаючи нові технологічні розробки та зміни в ринкових потребах.

– Екологічний розвиток. Індустрія 5.0 наголошує на важливості циркулярних процесів, які сприяють переробці та повторному використанню природних ресурсів, зменшенню відходів та зниженню екологічного впливу, тим самим підвищуючи ефективність виробничих процесів[4].

За іншим підходом, кібербезпека полягає в захисті від кібератак, які націлені на корпоративні мережі[5]. Л. Бєлкін, Ю. Юринець, М. Бєлкін, Є. Криволап доводять, що кібербезпека є окремим випадком загального поняття безпеки інформації, але такої інформації, яка обертається у кіберпросторі. При цьому причиною підвищеної уваги саме до кіберзагрозам і кібербезпеки є дедалі зростаюча роль обігу інформації в комп'ютерних системах і електронно-комунікаційних мережах. Та пропонують ввести у стабільний науковий і практичний оборот поняття «когнітивна безпека» як стійкість проти інформаційно-психологічних впливів на людину і суспільство[6].

Г. Форос та В. Жогов в одній зі своїх публікацій наголошують на двох підходах до поняття кібербезпека: вузькому та широкому. При розгляді кібербезпеки у вузькому значенні, на думку науковців, необхідно говорити, перш за все про захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. У широкому сенсі, їхнє бачення полягає в тому, що кібербезпека – це сукупність вольових суспільних відносин, що складаються в процесі свідомого

[4] Попова Д. В. Кібербезпека в епоху Індустрії 5.0: нові виклики та можливості. *Економічний вісник Донбасу.* 2024. № 3. С. 203-216. DOI: https://doi.org/10.12958/1817-3772-2024-3(77)-203-216

[5] Кострома М. О. Кіберстійкість і кібербезпека: у чому різниця? *Сучасний захист інформації.* 2022. № 4. С. 71-75. DOI: 10.31673/2409-7292.2022.040012

[6] Бєлкін Л. М. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020-2021 років. *Юридичний вісник. Повітряне і космічне право*. 2022. № 3. С. 78-86. DOI: 10.18372/2307-9061.64.16893

і добровільного дотримання громадянами встановлених в нормах права та в інших нормах неюридичного характеру правил поведінки в кіберпросторі, і тим самим забезпечуються злагоджене, стійке, спільне життя людей в умовах розвинутого суспільства[7].

І. Яковів вважає, що ключовим терміном для розуміння сутності «кібербезпеки» є «кіберпростір». Зазвичай його пов'язують з: глобально розподіленими системами, що реалізовують цифрові комп'ютерні технології обробки інформації; віртуальним середовищем на основі цих систем, в якому можуть існувати видумані активні об'єкти (різноманітні герої комп'ютерних ігор і цифрової анімації, симуляційні моделі та інше). Ці інформаційні об'єкти, що існують тільки в комп'ютерах, здатні здійснювати реальний сенсорний вплив на психіку людини (візуальний, звуковий та іншій); можливістю здійснювати приховані (анонімні) інформаційні впливи на людей і різні пристрої; відсутністю «територіальних кордонів» при комунікаціях людей різних держав (відсутність «кіберкордонів»)[8].

У науковому доробку О. Ткаченка та К. Ткаченко представлена комплексна дефініція ключових категорій сфери цифрової безпеки, зокрема понять «кіберпростір», «кібербезпека» та «забезпечення кібербезпеки». Автори пропонують розглядати кіберпростір як специфічне кіберінформаційне середовище, що акумулює в собі семантичну сутність об'єктів профільної інфраструктури, а також архітектуру взаємозв'язків між ними. У межах цієї концепції об'єкти кіберінформаційної інфраструктури диференціюються на три засадничі рівні: апаратно-технічний (кінцеве обладнання, гаджети, персональні обчислювальні машини); програмно-технологічний (мережева інфраструктура та відповідне програмне забезпечення); інформаційний (бази даних, вебконтент та масиви інтернет-відомостей). Під кібербезпекою дослідники розуміють динамічний стан захищеності кіберпростору держави та його структурних елементів від деструктивного зовнішнього впливу. Такий стан характеризується мінімізацією ризиків порушення стабільності системи та її сталого розвитку. Ключовим аспектом кібербезпеки в інтерпретації авторів є здатність до своєчасної ідентифікації, превенції та нейтралізації кіберзагроз і кіберзлочинів, що можуть загрожувати інтересам особи, корпоративного сектору, державних інституцій чи національній безпеці загалом. Логічним продовженням цієї концепції є дефініція забезпечення кібербезпеки, яке трактується як цілеспрямована сукупність заходів, орієнтованих на редукцію ризиків заподіяння шкоди внаслідок технічних збоїв, програмних помилок або несанкціонованого (некоректного) використання ресурсів кіберпростору. Крім

[7] Форос Г. В. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава.* 2019. № 33. С. 128-134. DOI: https://doi.org/10.18524/2411-2054.2019.33.162068

[8] Яковів І. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека. *Information Technology and Security*. 2017. Vol. 5, № 2. С. 134-144. DOI: https://doi.org/10.20535/2411-1031.2017.5.2.136981

того, цей процес охоплює заходи з оперативного відновлення функціональності всіх складових кіберінфраструктури після настання деструктивних подій[9].

2. Законодавче регулювання кібербезпеки в Україні: аналіз імплементації та стратегічних напрямків

Оскільки кібербезпека стала національним пріоритетом, відповідальність за розробку та реалізацію політики кібербезпеки була чітко розподілена в державному секторі. Однак жоден з існуючих органів влади не має комплексного розуміння та достатньо широкого мандату для управління всіма аспектами кібербезпеки. В. Дзюндзюк та Є. Котух виділяють низку загальних аспектів, які, на їх погляд, мають бути присутніми в політиці та стратегії кібербезпеки в Україні. Зокрема, це: урахування питань суверенітету при розробці політики; важливість діалогу за участю багатьох зацікавлених сторін; важливість економічних аспектів кібербезпеки; покращення міжнародного співробітництва; гнучкий підхід до формування та реалізації політики; повага до фундаментальних цінностей; посилення координації органів влади на політичному та оперативному рівнях; зміцнення публічно-приватного співробітництва[10].

Окремі питання кіберзахисту містяться в Кодексі цивільного захисту України, в Законах України «Про інформацію», «Про захист інформації в інформаційно-комунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про критичну інфраструктуру». В постановах Кабінету Міністрів України: Про затвердження Порядку оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури (від 31.12.2025 № 1799), Про затвердження Порядку здійснення державного контролю за додержанням вимог законодавства у сфері кіберзахисту (від17.12.2025 № 1668), Деякі питання пошуку та виявлення потенційних вразливостей в інформаційно-комунікаційних системах (від 03.12.2025 № 1580), Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози (від 26.11.2025 № 1533), Про затвердження Порядку призначення керівника з кіберзахисту на посаду в органі державної влади (від 26.11.2025 № 1516) та ін.

Послідовність у намірах законодавця прослідковується з 2016 року. Зокрема з затвердження Стратегії кібербезпеки України, що стала важливим кроком у запровадженні підходів довгострокового планування в цій сфері. Метою Стратегії кібербезпеки України (2016 року) стало створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Для досягнення цієї мети необхідними було: створення національної системи кібербезпеки; посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю,

[9] Ткаченко О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2018. Вип. 1. С. 75-86. DOI: https://doi.org/10.31866/2617-796x.1.2018.147257

[10] Дзюндзюк В. Б. Кібербезпека як один з пріоритетів національної політики. *Державне будівництво*. 2020. № 2. С. 1-19. DOI: 10.34213/db.20.02.01

поглиблення міжнародного співробітництва у цій сфері; забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України, та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура)[11].

У 2017 році був прийнятий Закон України «Про основні засади забезпечення кібербезпеки України». Закон визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. У ст. 1 законодавець тлумачить такі терміни як: індикатори кіберзагроз, інформація про інцидент кібербезпеки, інцидент кібербезпеки, кібератака, кіберзагроза, кіберзахист, кіберзлочин, кіберзлочинність, кібероборона, кіберпростір, кіберрозвідка, кібертероризм, кібершпигунство та інші. Зокрема, законодавець термін кібербезпека трактує як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі[12]. Відповідно до ст. 4 Закону об'єктами кібербезпеки є: 1) конституційні права і свободи людини і громадянина; 2) суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; 3) держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; 4) національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; 5) об'єкти критичної інфраструктури. Об'єктами кіберзахисту визначені: 1) комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; 2) об'єкти критичної інформаційної інфраструктури; 3) комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу[13].

[11] Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836 (дата звернення: 14.02.2026).

[12] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2026).

[13] Там само.

Нова Стратегія кібербезпеки України (2021 року) врахувала попередній досвід і проблеми, стан кібербезпекового середовища на національному та міжнародному рівні, а також положення Стратегії кібербезпеки ЄС на цифрове десятиліття, стратегій кібербезпеки окремих держав – членів ЄС та держав – членів НАТО. Були визначені нові загрози кібербезпеці України: гібридна агресія Російської Федерації проти України у кіберпросторі; кіберзлочинність, що завдає шкоди інформаційним ресурсам, суспільним процесам, особисто громадянам, знижує довіру суспільства до інформаційних технологій та призводить до значних матеріальних втрат; організовані та спонсоровані урядами інших держав кібератаки, що пов'язані з викраденням у політичних, економічних або військових цілях чутливої інформації (кібершпигунство) та здійсненням розвідувально-підривної діяльності; використання терористичними організаціями кіберпростору для вчинення актів кібертероризму, фінансової та іншої підтримки терористичної діяльності. Відповідно визначені передумови та чинники, які формують окреслені загрози:

– висока технологічна залежність України від іноземних виробників продукції інформаційно-комунікаційних технологій, відсутність системи оцінки відповідності такої продукції вимогам з безпеки, що підвищує ступінь уразливості інформаційної інфраструктури від незадекларованих функцій та звужує спроможності протидії кіберзагрозам;

– недосконалість нормативно-правової бази у сфері кібербезпеки, а також її застарілість у сфері захисту інформації, повільна імплементація положень європейського законодавства, недостатня врегульованість цифрової складової розслідування кримінальних правопорушень, а також низький рівень правової відповідальності за порушення вимог законодавства у цій сфері;

– відсутність у значної частини державних органів відповідних структурних підрозділів, необхідного кадрового забезпечення та належного контролю за кіберзахистом, здійснення фінансування робіт із кіберзахисту за залишковим принципом;

– відсутність системи незалежного аудиту інформаційної безпеки та механізмів розкриття інформації про вразливості в умовах динамічної цифровізації всіх сфер державного управління та життєдіяльності держави;

– невідповідність сучасним вимогам рівня підготовки та підвищення кваліфікації фахівців з питань кібербезпеки та кіберзахисту, зокрема неефективні механізми їх стимулювання до роботи в державному секторі;

– відсутність законодавчого акта про критичну інфраструктуру України та її захист, що значно ускладнює формування системи кіберзахисту такої інфраструктури;

– незавершеність заходів з упровадження організаційно-технічної моделі кіберзахисту, яка відповідатиме сучасним загрозам, викликам у кіберпросторі та глобальним тенденціям розвитку індустрії кібербезпеки;

– відсутність дієвої системи інформаційно-аналітичного забезпечення кібербезпеки;

– недостатня захищеність від кібератак державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури;

– невідповідність вимогам законодавства стану захисту інформаційно-комунікаційних систем державних органів та суб'єктів господарювання, в яких обробляється значна частина інформації з обмеженим доступом;

– відсутність системи підвищення цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, низький рівень обізнаності суспільства щодо кіберзагроз та кіберзахисту[14].

Для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є: посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування); набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість); забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами – членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія)[15].

Згодом затверджено план заходів на 2025 рік з реалізації Стратегії кібербезпеки України. У таблиці Плану Урядом було визначено 29 завдань. Зокрема такими є: створення в системі Міноборони кібервійськ, забезпечення їх належними фінансовими, кадровими та технічними ресурсами для стримування збройної агресії в кіберпросторі та надання відсічі агресору; запровадження ефективних механізмів взаємодії основних суб'єктів національної системи кібербезпеки та сил оборони в частині спільного виконання завдань кібероборони; розроблення та забезпечення виконання плану кібероборони як складової частини плану оборони України; посилення спроможностей щодо проведення негласних перевірок стану готовності об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів, поступове охоплення такими заходами всіх об'єктів; посилення контррозвідувального захисту сфери електронних комунікацій, ІТ-сфери, афілійованого з ними середовища, що спрямований на виявлення, попередження і припинення розвідувально-підривних посягань спецслужб іноземних держав на національну безпеку у сфері кібербезпеки[16].

[14] Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021 (рішення РНБО від 14.05.2021). URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 14.02.2026).

[15] Там само.

[16] Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 07.03.2025 № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text (дата звернення: 14.02.2026).

3. Класифікація та механізми управління кіберінцидентами: синергія наукових підходів та державних стандартів

Дослідження української наукової спільноти демонструють еволюцію від теоретичного осмислення кіберзахисту до розробки прикладних методик протидії в умовах реальної кібервійни. Аналіз праць провідних фахівців дозволяє виокремити ключові вектори розвитку вітчизняної наукової думки щодо класифікації та управління кіберінцидентами. Праці Є. Живила та І. Ромашки зосереджені на створенні системних протоколів спільної дії. Їхній підхід підкреслює важливість злагодженої взаємодії різних суб'єктів кібербезпеки не лише під час атаки, а й у процесі ліквідації її наслідків, що фактично формує операційну основу для державної системи реагування[17]. В. Федик та Г. Денисенко акцентують увагу на захисті об'єктів критичної інфраструктури. Їхні дослідження класифікують інциденти крізь призму менеджменту кризових ситуацій, пропонуючи методологію, де реагування є невід'ємною частиною загальної стратегії управління ризиками[18]. Питання вимірюваності успіху команд реагування піднімають В. Кінзерявий та В. Гнатюк. Встановлення базових показників ефективності дозволяє об'єктивно оцінювати спроможність підрозділів і класифікувати їх за рівнем готовності до відбиття загроз[19]. О. Сахарова та І. Близнюк розглядають виявлення інцидентів як стратегічний інструмент запобігання кіберзлочинності. Їхня позиція інтегрує технічні заходи реагування у загальну правову рамку боротьби зі злочинністю в цифровому просторі[20]. Сучасним доповненням до технічних аспектів є робота О. Гарасимчука, Т. Костишина, О. Любчика та М. Швед, які фокусуються на розробці методик оповіщення населення. Це розширює класичне розуміння реагування, виводячи його за межі вузькоспеціалізованих ІТ-департаментів у площину суспільної безпеки[21].

На думку А. Вавіленко залежно від характеру та масштабів кіберінциденти можуть бути класифіковані так: 1) інциденти низької важливості – мінімальний вплив на систему, який не призводить до серйозних наслідків; 2) серйозні інциденти – інциденти, які суттєво впливають на функціонування системи або можуть спричинити витоки конфіденційних даних; 3) критичні інциденти –

---

[17] Живило Є. О. Протокол спільних дій суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти, а також при усуненні їх наслідків. *Системи управління, навігації та зв'язку.* 2024. Вип. 1. С. 66-76. DOI: 10.26906/SUNZ.2024.1.066

[18] Федик В. Р. Теоретико-методологічні підходи до управління ризиками кібербезпеки на об'єктах критичної інфраструктури: реагування на кіберінциденти та менеджмент кризових ситуацій. *Інформація і право.* 2024. № 1. С. 195-202. DOI: 10.37750/2616-6798.2024.1(48).300822

[19] Кінзерявий В. Базові показники ефективності роботи команд реагування на кіберінциденти. *Безпека інформації.* 2014. Т. 20, № 2. С. 193-196.

[20] Сахарова О. Б. Виявлення та реагування на кіберінциденти і кібератаки як заходи запобігання кіберзлочинності. *Наука і правоохорона*. 2023. Вип. 2. С. 220-231. DOI (Issue): https: //doi.org/10.36486/np.2023.2(60)

[21] Гарасимчук О. І. Розробка вдосконаленої методики оповіщення населення про кіберінциденти. *Інформатика та математичні методи в моделюванні.* 2025. Т. 15, № 2. С. 187-195. DOI 10.15276/imms.v15.no2.187

інциденти, що мають великий масштаб і можуть призвести до значних фінансових або репутаційних втрат для організації[22].

Чотирирівнева модель класифікації інцидентів, запропонована О. Саморай та О. Семенюк, становить методологічну базу для комплексного аналізу потенційних деструктивних впливів. Поділ загроз на технічні, соціальні, фізичні та інциденти безпеки дозволяє сформувати цілісну архітектуру моніторингу та обрати найбільш релевантні стратегії детекції й алгоритми реагування для кожного специфічного сценарію. Такий структурований підхід забезпечує високу адаптивність систем захисту до різнопланових викликів сучасної IT-інфраструктури. Розглянемо кожен із зазначених рівнів детальніше. Технічні інциденти становлять категорію деструктивних подій, зумовлених апаратними чи програмними деградаціями, що призводять до дестабілізації або повної зупинки роботи інформаційних систем. Етіологія таких збоїв зазвичай охоплює широкий спектр чинників, серед яких першочергове значення мають критичні несправності фізичного обладнання – серверної інфраструктури, накопичувачів даних та мережевих вузлів. Поряд із цим суттєвий ризик становлять недосконаліть програмного коду, наявність уразливостей, а також виникнення міжаплікаційних конфліктів або помилок під час оновлення систем через їхню технологічну несумісність. Окрему групу чинників формують порушення в роботі комунікаційних каналів, що включають відмови маршрутизаторів, перевантаження ліній зв'язку та низьку експлуатаційну якість послуг інтернет-провайдерів. Крім того, критичний вплив на доступність ресурсів мають цілеспрямовані DDoS-атаки, механізм яких полягає у штучному створенні масового потоку запитів для вичерпання лімітів системи, що неминуче спричиняє часткову або повну відмову в обслуговуванні користувачів[23]. Інциденти безпеки класифікуються як події, що несуть пряму загрозу цілісності, доступності та конфіденційності інформаційних активів, потенційно призводячи до несанкціонованого витоку або ексфільтрації даних. Спектр таких інцидентів охоплює компрометацію облікових записів користувачів шляхом ініціації атак типу «brute-force» (підбір паролів) або експлуатацію системних уразливостей для несанкціонованого проникнення в периметр корпоративних і державних мереж. Додатковим аспектом є деструктивні дії, спрямовані на копіювання, несанкціоновану публікацію чи передачу критично важливих відомостей третім особам. Суттєву роль у структурі таких загроз відіграє впровадження шкідливого програмного забезпечення – вірусів, троянських програм та криптолокерів (програм-вимагачів), що здатні зашифровувати інформаційні масиви з метою шантажу або встановлювати повний адміністративний контроль над інфікованою системою[24]. Соціальні інциденти становлять категорію загроз, що реалізуються

[22] Вавіленко А.І. Процес управління кіберінцидентами як необхідний етап в організації кібербезпеки підприємства. *Інформаційна безпека людини, суспільства, держави*. 2025. № 1 (38). С.64-71. DOI: 10.511369/2707-7276-2025-1(38)-6

[23] Саморай О.К., Семенюк О.О. Теоретичні і практичні підходи до розуміння кіберінцидентів та їхньої ідентифікації. *Європейський правничий часопис.* 2025. Вип. 8. С. 56-62. DOI 10.36919/3041-1149 (Print).8.2025.56-62

[24] Там само.

через методи цілеспрямованого психологічного впливу на суб'єктів інформаційних відносин для отримання несанкціонованого доступу до конфіденційних активів. Ключовим інструментарієм таких атак є фішинг – розсилка фальсифікованих електронних листів або повідомлень, які імітують верифіковані офіційні джерела з метою ексфільтрації облікових даних користувачів. Окреме місце займають різноманітні техніки соціальної інженерії, що базуються на прямій маніпуляції свідомістю для компрометації систем або викрадення інформації. Це може відбуватися через нав'язливу телефонну комунікацію (вішинг), створення шахрайських запитів або застосування методів обману в соціальних медіа, де зловмисники використовують когнітивні упередження та довіру користувачів для подолання встановлених протоколів безпеки. Фізичні інциденти класифікуються як події, наслідком яких є матеріальна деградація, механічне пошкодження або безпосередня втрата елементів інформаційних систем, мережевої інфраструктури та фізичних носіїв даних. Найбільш критичними проявами таких інцидентів є акти незаконного відчуження або навмисного знищення апаратних засобів, зокрема крадіжки мобільних робочих станцій, серверних модулів чи накопичувачів інформації. Суттєвий деструктивний потенціал мають також природні чинники форс-мажорного характеру – повені, пожежі, сейсмічна активність та інші катаклізми, здатні спричинити масштабні руйнування серверних приміщень і центрів обробки даних. Крім того, до цієї категорії відносять критичні збої в допоміжних інженерних системах, таких як модулі електроживлення або кондиціонування. Порушення регламентних умов експлуатації призводить до термічного перевантаження серверів, що тягне за собою апаратну відмову компонентів або безповоротну втрату цифрових масивів даних[25].

У науковому середовищі підхід до виявлення та аналізу кіберзагроз часто базується на гнучких евристичних моделях та предиктивній аналітиці, де головна увага приділяється динамічній природі атак і пошуку інноваційних методів захисту. Натомість законодавець оперує категоріями жорсткої регламентації та правової визначеності, фокусуючись на встановленні чіткої таксономії, часових лімітів інформування та суворого розподілу відповідальності між суб'єктами кібербезпеки. Таким чином, якщо науковці прагнуть розширити межі пізнання механізмів загроз, то правотворча позиція спрямована на створення стабільного, юридично значущого протоколу, що забезпечує невідворотність реагування в масштабах усієї держави.

Постановою Кабінету Міністрів України «Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози» від 26 листопада 2025 р. № 1533 було затверджено: Національний план реагування на кіберінциденти, кібератаки та кіберзагрози; критерії віднесення інформації про характер, технічні та інші деталі кіберінциденту, кібератаки до інформації з обмеженим доступом, перелік підстав, порядок та мету розкриття такої інформації; Порядок публічного інформування або звітування про реагування на кіберінциденти, кібератаки, усунення їх

[25] Саморай О.К., Семенюк О.О. Теоретичні і практичні підходи до розуміння кіберінцидентів та їхнбої ідентифікації. *Європейський правничий часопис.* 2025. Вип. 8. С. 56-62. DOI 10.36919/3041-1149 (Print).8.2025.56-62

наслідків.[26] Зокрема у Національному плані законодавець визначив загальні процедури реагування на кіберінциденти, кібератаки, кіберзагрози, а також механізм координації та взаємодії між суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та суб'єктами забезпечення кібербезпеки, їх роль в рамках функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози та національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози. Дія цього Національного плану поширюється на основних суб'єктів національної системи кібербезпеки, суб'єктів національної системи реагування, органи державної влади, державні органи, органи місцевого самоврядування, операторів критичної інфраструктури, власників або розпорядників об'єктів критичної інформаційної інфраструктури, інших суб'єктів забезпечення кібербезпеки, які відповідно до законодавства залучені до виконання завдань в рамках функціонування національної системи реагування. Окрім цього, законодавець розкриває такі поняття як: власна команда реагування на кіберінциденти, кібератаки та кіберзагрози (CSIRT); підрозділ з кіберзахисту; подія кібербезпеки; ризик кібербезпеки[27].

Процес протидії кіберзагрозам, атакам та інцидентам ініціюється стадією підготовки, у межах якої суб'єкти національної системи кібербезпеки здійснюють фундаментальні дослідження наявних типів кіберзагроз та розробляють превентивні механізми захисту. Цей етап передбачає формування комплексу організаційних, технічних і кадрових умов, необхідних для оперативного та результативного відбиття загроз. Зокрема, суб'єкти забезпечують системне планування заходів реагування, ґрунтуючись на результатах безперервного управління кіберризиками. Важливим аспектом є налагодження чіткої вертикальної та горизонтальної взаємодії між керівниками напрямів кіберзахисту, профільними підрозділами, внутрішніми командами реагування (CSIRT) та загальнодержавними структурами. Нормативна база підготовки включає розробку та постійну актуалізацію стандартних операційних процедур (SOP) для різних сценаріїв атак, що базуються на методичних рекомендаціях Адміністрації Держспецзв'язку. Окрему увагу приділено освітньому компоненту: організації диференційованого навчання персоналу, програма якого адаптується під функціональні ролі та професійну кваліфікацію співробітників. Технічна складова підготовчого етапу реалізується через створення необхідної інфраструктури для інтеграції локальних систем із державними технічними засобами реагування, зокрема через підключення до централізованої системи Державного центру кіберзахисту Держспецзв'язку[28].

Етап виявлення та аналізу базується на безперервному моніторингу систем для ідентифікації аномальної активності та індикаторів компрометації. Процес реагування активується як внутрішніми службами безпеки, так і через державні платформи обміну даними. У разі підтвердження інциденту суб'єкти безпеки

[26] Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Кабінету Міністрів України від 26.11.2025 № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text (дата звернення: 14.02.2026).

[27] Там само.

[28] Там само.

спільно з CERT-UA або профільними командами CSIRT класифікують його за національною таксономією та визначають рівень критичності: від 0 (білий) – некритичний, до 5 (чорний) – надзвичайний, що загрожує життю людей або функціонуванню держави. Процес інформування здійснюється в режимі реального часу через принцип «єдиного вікна» та платформу MISP-UA (керовану СБУ), з обов'язковим дотриманням протоколу конфіденційності TLP. Для об'єктів критичної інфраструктури та держустанов встановлено жорсткий регламент: повідомлення про значні інциденти має бути надіслане протягом однієї години. Подальша звітність перед Національним координаційним центром кібербезпеки передбачає чіткі часові межі: попередній звіт – 24 години, поточний – 72 години, та фінальний – протягом місяця. Це забезпечує злагоджену координацію між приватними, галузевими та національними центрами кіберзахисту для оперативної локалізації загроз[29].

4. Взаємодія суб'єктів забезпечення кібербезпеки щодо фіксації цифрових доказів та нейтралізації кіберінцидентів: емпіричний аналіз діяльності органів правопорядку

Відповідно до ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України. Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та загальний контроль за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, загальну координацію суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози; подає до Ради національної безпеки і оборони України пропозиції щодо оголошення кризової ситуації в кібербезпеці; координує реалізацію Стратегії кібербезпеки України, подає до Ради національної безпеки і оборони України пропозиції щодо формування та уточнення Стратегії, у тому числі з урахуванням положень Директиви Європейського Союзу щодо мережевої та інформаційної безпеки (NIS 2 Directive); визначає пріоритети, розробляє концептуальні засади та вносить Президентові України пропозиції щодо проведення кібероперацій стратегічного рівня в інтересах національної безпеки і оборони та забезпечує координацію суб'єктів сектору безпеки і оборони щодо їх проведення; координує стратегічні комунікації у сфері кібербезпеки[30].

Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю;

[29] Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Кабінету Міністрів України від 26.11.2025 № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text (дата звернення: 14.02.2026).

[30] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2026).

організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; затверджує національний план реагування; затверджує загальні вимоги з кіберзахисту об'єктів критичної інфраструктури; затверджує порядок оцінювання стану кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем, в яких обробляються державні інформаційні ресурси або службова інформація та інформація, що становить державну таємницю, об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури (крім систем та об'єктів банків); встановлює порядок взаємодії суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози із суб'єктами забезпечення кібербезпеки, з правоохоронними, контррозвідувальними, розвідувальними органами та суб'єктами оперативно-розшукової діяльності[31].

Суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, є: міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування; Національний банк України; оператори критичної інфраструктури та власники або розпорядники об'єктів критичної інформаційної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом[32].

Суб'єкти забезпечення кібербезпеки у межах своєї компетенції: здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підривних, терористичних та інших протиправних і злочинних цілях; здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту; забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору[33].

Інституційне забезпечення кібербезпеки на рівні державних інституцій та критичної інфраструктури реалізується через обов'язкове створення профільних структурних одиниць – підрозділів з кіберзахисту. Законодавець у ст. 5-1 Закону «Про основні засади забезпечення кібербезпеки України» встановлює вимогу для органів державної влади, які оперують державними інформаційними ресурсами або таємною інформацією, не лише формувати такі підрозділи, а й призначати керівників з кіберзахисту з прямим підпорядкуванням.

[31] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2026).

[32] Там само.

[33] Там само.

Аналогічні функції в органах місцевого самоврядування та на об'єктах критичної інформаційної інфраструктури покладаються на спеціально призначених відповідальних осіб. Особлива увага приділяється процедурі кадрового відбору: призначення керівника з кіберзахисту в державному секторі потребує обов'язкового погодження з Держспецзв'язку та проходження перевірки з боку Служби безпеки України. При цьому діє механізм «мовчазної згоди», якщо вмотивована відмова не була надана протягом місяця. Функціональне навантаження таких керівників передбачає здійснення безперервного керівництва, координації та контролю заходів кіберзахисту, що залишається незмінним пріоритетом навіть в умовах правового режиму воєнного стану. Це підкреслює стратегічну роль управлінської ланки у забезпеченні стійкості інформаційних систем до критичних впливів[34].

Відповідно до ст. 8 Закону національна система кібербезпеки України розглядається як багатоаспектна екосистема, що інтегрує широку сукупність суб'єктів та взаємоузгоджених заходів для комплексного захисту цифрового суверенітету. Її архітектура охоплює не лише технічні та інженерні рішення, а й заходи політичного, наукового, освітнього та правового характеру. Окреме місце в структурі системи посідає реалізація специфічних державних функцій: оперативно-розшукової, розвідувальної та контррозвідувальної діяльності, а також оборонних стратегій. Такий підхід забезпечує надійний криптографічний і технічний захист національних інформаційних активів та гарантує кіберстійкість об'єктів критичної інформаційної інфраструктури[35].

Координація зусиль у цій сфері покладається на ключових суб'єктів національної системи кібербезпеки, кожен з яких діє в межах визначеної законом компетенції. До основного інституційного ядра належать Державна служба спеціального зв'язку та захисту інформації, Служба безпеки України, Національна поліція, Міністерство оборони разом із Генеральним штабом ЗСУ, а також розвідувальні органи. Окрім силового та технічного блоку, до системи інтегровані Національний банк України та Міністерство закордонних справ, що дозволяє забезпечувати економічну стабільність та дипломатичну підтримку кіберзахисту на міжнародній арені. Така розгалужена структура суб'єктів забезпечує цілісність державного реагування на кіберзагрози будь-якого рівня складності.

Ефективність функціонування національної системи кібербезпеки безпосередньо залежить від спроможності правоохоронних органів та суб'єктів державного контролю здійснювати кваліфікований збір, фіксацію та аналіз цифрових доказів. Провідна роль у цьому процесі належить Департаменту кіберполіції Національної поліції України, який забезпечує процесуальне супроводження кіберінцидентів у межах кримінального судочинства. Діяльність цього підрозділу спрямована на виявлення індикаторів компрометації (IoC) та вилучення цифрових слідів за допомогою спеціалізованих програмно-апаратних комплексів, що гарантують збереження автентичності даних через створення дзеркальних образів носіїв інформації. Важливою складовою є легалізація

[34] Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2026).

[35] Там само.

технічних параметрів атаки, де результати криміналістичного аналізу (forensics) трансформуються у юридично значущу доказову базу, що відповідає критеріям допустимості та цілісності.

Аналіз практичної діяльності Департаменту кіберполіції Національної поліції України у 2024 році свідчить про перехід до стратегії активного наступального протистояння загрозам у цифровому просторі. У звітному періоді зусилля підрозділу були зосереджені на превенції, детекції та нейтралізації кіберінцидентів, що підтверджується вагомими статистичними показниками оперативно-службової діяльності. Емпіричні дані вказують на високу інтенсивність боротьби з консолідованими злочинними угрупованнями. Зокрема, у 2024 році було ліквідовано 57 організованих груп, з яких 9 складали злочинні організації. До кримінальної відповідальності притягнуто 254 учас-ники, чия деструктивна діяльність охоплювала понад 1 000 епізодів. Загальна динаміка процесуальної діяльності ДКП за рік характеризується наступними показниками: реєстрація 2,5 тис. кіберзлочинів; оголошення про підозру 1,7 тис. особам у вчиненні 3,5 тис. правопорушень; завершення досудового розслідування у 4,4 тис. провадженнях; направлення до суду обвинувальних актів щодо понад 4 тис. злочинів. Ефективність функцій відшкодування збитків демонструє позитивну тенденцію: потерпілим забезпечено повернення понад 168,6 млн грн, що становить 42,5% від загальної суми завданої матеріальної шкоди.

Дослідження виявило адаптацію кіберзлочинності до актуальних соціальних трендів. Специфічними для періоду воєнного стану стали правопорушення, пов'язані з наданням фіктивних послуг чоловікам призовного віку, фальсифікацією волонтерської допомоги та шахрайством у сфері оренди житла для ВПО. У цьому сегменті правоохоронцями ідентифіковано та повідомлено про підозру понад 700 особам, а щодо 620 осіб матеріали передано до суду. В межах міжвідомчої взаємодії з НБУ та Держспецзв'язку було реалізовано механізм масового обмеження доступу до доменних імен, задіяних у фішингових кампаніях та соціальній інженерії.

Сучасний рівень інтеграції ДКП у світову архітектуру кібербезпеки підтверджується участю у 17 масштабних міжнародних поліцейських операціях, проведених спільно з іноземними партнерами та Європолом. Результатом став демонтаж інфраструктури кількох транснаціональних хакерських об'єднань. Важливим кроком у межах реалізації Стратегії кібербезпеки України стало отримання доступу до комунікаційної системи «Інтерпол I-24/7», що прискорило транскордонний обмін цифровими доказами.

Особливого значення набула екосистема «BRAMA», створена за координації кіберполіції як приклад державно-приватного партнерства. Проєкт об'єднав волонтерів та IT-фахівців для блокування ворожих джерел дезінформації. Ефективність платформи підтверджується динамікою охоплення аудиторії: на кінець 2024 року кількість активних підписників каналу протидії ворожому контенту досягла майже 148 тисяч осіб.

Таким чином, результати 2024 року підтверджують роль Департаменту кіберполіції як суб'єкта, що забезпечує не лише кримінально-правове переслідування зловмисників, а й безперервний моніторинг національних

комунікаційних мереж у режимі реального часу, інтегруючи сучасні технологічні рішення в архітектуру національної безпеки[36].

Паралельно з поліцейським блоком, органи державного контролю, зокрема Державна служба спеціального зв'язку та захисту інформації України, виконують роль первинної ланки технічного реагування. Через Державний центр кіберзахисту та команду CERT-UA здійснюється моніторинг об'єктів критичної інфраструктури, фіксація лог-файлів та встановлення методичних стандартів збереження цифрової інформації. У випадках, коли кіберінцидент загрожує національній безпеці або територіальній цілісності, до процесу долучається Служба безпеки України. Її функції зосереджені на контррозвідувальній атрибуції атак, що дозволяє ідентифікувати причетність іноземних спецслужб або APT-угруповань. Координація між цими суб'єктами базується на принципі «ланцюжка зберігання» (chain of custody), де технічні дані, зібрані під час моніторингу, стають основою для експертних висновків. Таким чином, синергія правоохоронних та контролюючих органів створює надійний механізм використання електронних доказів, що забезпечує невідворотність відповідальності за правопорушення у кіберпросторі.

Сучасний етап гібридної агресії проти України характеризується подальшою ескалацією в кіберпросторі, що підтверджується даними аналітичного звіту Державної служби спеціального зв'язку та захисту інформації України за перше півріччя 2025 року. Ключовою особливістю звітного періоду стала висока ступінь координації кібероперацій із конвенційними військовими діями, зокрема ракетно-дроновими ударами по об'єктах інфраструктури, що свідчить про інтеграцію цифрових атак у загальний стратегічний задум противника. Протягом першої половини 2025 року зафіксовано 3 018 кіберінцидентів, що відображає зростання інтенсивності на 17% порівняно з другим півріччям 2024 року. В аспекті якісної оцінки спостерігається трансформація структури інцидентів: при загальному збільшенні кількості атак середнього рівня критичності зафіксовано зниження частки критичних та високих інцидентів. Така тенденція є прямим наслідком превентивного посилення національних систем кіберзахисту. Розподіл цілей кібератак демонструє пріоритетність впливу на систему державного управління та сектор безпеки. Найбільшого деструктивного тиску зазнали: органи місцевого самоврядування – 34%; сектор безпеки та оборони – 23%; урядові організації та центральні органи виконавчої влади – 19%. У структурі використовуваного інструментарію домінують фішинг (27%), інфікування шкідливим програмним забезпеченням (21%) та компрометація облікових записів (5,4%). Характерною ознакою звітного періоду стало використання високотехнологічних методів проникнення хакерськими угрупованнями, афілійованими з ГУ ГШ ЗС РФ. Зокрема, зафіксовано активну експлуатацію Zero-Click вразливостей, які не потребують взаємодії з користувачем для інфікування системи. Основними векторами атак залишаються поштові платформи Roundcube та Zimbra, а також використання легітимних хмарних сервісів (Dropbox, Google Drive, Cloudflare)

[36] Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році : звіт від 31.01.2025. Офіційний сайт Кіберполіції України. URL: https://cyberpolice.gov.ua/news/zvit-pro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/ (дата звернення: 17.02.2026).

для прихованої доставки шкідливого контенту[37]. Окрему наукову увагу привертає зафіксоване CERT-UA використання технологій штучного інтелекту для генерації адаптивних фішингових повідомлень та автоматизації розробки експлуатаційного коду. Це свідчить про якісний стрибок у технологічній оснащеності суб'єктів кіберагресії. Незважаючи на зростаючу інтенсивність викликів, рівень резистентності державних і приватних інституцій продемонстрував стійку позитивну динаміку.

Фундаментом для цих змін стала імплементація положень Закону України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури», що регламентує розбудову мережі регіональних та секторальних команд реагування (CSIRT). Важливим етапом інституційної трансформації стало реформування CERT-UA у статус національного CSIRT, що забезпечило централізацію координаційних процесів та підвищило оперативність реагування на значні кіберінциденти[38].

ВИСНОВКИ

Дослідження продемонструвало, що в сучасних умовах «пермакриз» кібербезпека трансформувалася з вузькотехнічної дисципліни у багатоаспектне соціально-правове явище. Наукові підходи (зокрема концепції Індустрії 5.0 та когнітивної безпеки) акцентують увагу на захисті не лише інфраструктури, а й свідомості людини як головного об'єкта деструктивного впливу. Встановлено, що ключовим для розуміння галузі є трирівневе трактування кіберпростору (апаратний, програмний, інформаційний рівні), де безпека забезпечується через сталий розвиток і своєчасну нейтралізацію загроз на кожному з етапів.

Аналіз нормативної бази свідчить про системність зусиль держави у розбудові правового фундаменту кіберзахисту. Простежується перехід до жорсткої регламентації процедур реагування. Створення Національного плану реагування та запровадження обов'язкових посад керівників з кіберзахисту з прямим підпорядкуванням Держспецзв'язку та СБУ завершило формування вертикалі управління, що забезпечує стійкість державних інформаційних ресурсів навіть в умовах воєнного стану.

Емпіричні дані свідчать про експоненціальне зростання вітчизняного ринку кібербезпеки (з 32 млн дол. у 2016 р. до 138 млн дол. у 2024 р.). Україна перетворилася на глобальний R&D-полігон, де специфіка воєнного стану стимулювала домінування сегмента кіберрішень (57% ринку) над сервісами. Прогнозоване досягнення відмітки у 209 млн дол. до 2029 року та розвиток екосистем на кшталт «BRAMA» підкреслюють формування автономної та високотехнологічної індустрії, здатної забезпечити цифровий суверенітет держави в умовах глобального інформаційного протистояння.

[37] Фішинг, Zero Click-експлойти, AI-атаки: тенденції кіберзагроз в Україні у 2025 році. IT Ukraine. 07.10.2025. URL: https://itukraine.org.ua/fishing-zero-click-eksplojti-ai-ataki-tendentsiyi-kiberzagroz-v-ukrayini-u-2025-rotsi/ (дата звернення: 17.02.2026).

[38] Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 17.02.2026).

Узагальнення представлених теоретичних положень, нормативно-правового аналізу та емпіричних даних дозволяє сформулювати низку тез: 1. З огляду на активне використання AI для автоматизації атак і захисту, критично важливим є дослідження юридичних аспектів «автономної кібервійни». Пріоритетним є аналіз імплементації європейського AI Act у національне законодавство та розробка етичних протоколів застосування алгоритмів у діяльності правоохоронних органів. 2. Трансформація кіберзагроз у площину когнітивної війни (FIMI – Foreign Information Manipulation and Interference) вимагає перегляду класичних підходів. Наступні дослідження мають зосередитися на розробці методів захисту від маніпуляцій свідомістю, де цифрові технології використовуються як інструмент руйнування соціальної довіри. 3. Після законодавчого закріплення створення кібервійськ (кінець 2025 р.), актуальним стає наукове обґрунтування їхнього статусу, розробка доктрин ведення наступальних операцій у цифровому просторі та механізмів залучення «кіберрезерву» з-поміж цивільних фахівців. 4. Враховуючи масову цифровізацію та використання хмарних сервісів (Dropbox, Google Drive, Cloudflare) як векторів атак, перспективним є дослідження гармонізації національних стандартів безпеки IoT-пристроїв із міжнародними вимогами, що закладено в планах реагування. 5. Необхідно глибше дослідити механізми стимулювання вітчизняного ринку кібербезпеки. Пріоритетом є розробка моделей державно-приватного партнерства, де приватний сектор стає не лише постачальником послуг, а й інтегрованим елементом національної системи реагування. 6. Зважаючи на розвиток квантових обчислень, науковий інтерес становить перехід об’єктів критичної інфраструктури на постквантові алгоритми шифрування, що стане ключовим викликом для національної безпеки вже у найближчі роки.

АНОТАЦІЯ

Здійснено комплексне дослідження інституційних та правових засад функціонування національної системи кібербезпеки України. Проаналізовано еволюцію наукових підходів до дефініції ключових категорій галузі, зокрема понять «кіберпростір» та «кібербезпека», у контексті людиноцентричної парадигми та Індустрії 5.0. Особливу увагу приділено трансформації вітчизняного законодавства протягом 2016–2025 років, зокрема впровадженню Національного плану реагування на кіберінциденти та реформуванню CERT-UA у національний CSIRT. На основі актуальних емпіричних даних за 2024 та перше півріччя 2025 року висвітлено динаміку кібератак, проаналізовано роль Департаменту кіберполіції та Держспецзв’язку у забезпеченні цифрової стійкості держави. Деталізовано чотирирівневу модель класифікації кіберінцидентів та розкрито механізми збору цифрових доказів у межах кримінального судочинства. Виокремлено стратегічну роль державно-приватного партнерства та міжнародної співпраці через системи Інтерполу та Європолу. Обґрунтовано перспективи подальшого розвитку галузі, включаючи створення кібервійськ та імплементацію штучного інтелекту в архітектуру національної безпеки.

Література

1. Огляд ринку кібербезпеки в Україні : звіт / DataDriven, підкомітет з кібербезпеки EBA, CyberTech комітет Асоціації IT Ukraine за сприяння Аспен Інституту Київ, за підтримки Проєкту USAID. Січень 2025. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf (дата звернення: 10.02.2026).
2. Екзистенційні виклики перед Україною. Демографія. *DeepState*. 23.09.2023. URL: https://deepstateua.com/iekzistientsialni-vikliki-ukrayini-chastina-i-diemoghrafiia/ (дата звернення: 11.02.2026).
3. Бондаренко В. Кібербезпека: роль держави у захисті суспільства та окремої особистості у збереженні міжетнічного миру. *Аспекти публічного управління*. 2020. Т. 8, № Спец. вип. 1. С. 18–21. DOI: 10.15421/152031
4. Попова Д. В. Кібербезпека в епоху Індустрії 5.0: нові виклики та можливості. *Економічний вісник Донбасу*. 2024. № 3. С. 203–216. DOI: https://doi.org/10.12958/1817-3772-2024-3(77)-203-216
5. Костроміна М. О. Кіберстійкість і кібербезпека: у чому різниця? *Сучасний захист інформації*. 2022. № 4. С. 71–75. DOI: 10.31673/2409-7292.2022.040012
6. Бєлкін Л. М. Співвідношення понять «інформаційна безпека», «безпека інформації», «кібербезпека» в контексті безпекових стратегій України 2020–2021 років. *Юридичний вісник. Повітряне і космічне право*. 2022. № 3. С. 78–86. DOI: 10.18372/2307-9061.64.16893
7. Форос Г. В. Особливості трактування поняття «кібербезпека» в сучасній юридичній науці. *Правова держава*. 2019. № 33. С. 128–134. DOI: https://doi.org/10.18524/2411-2054.2019.33.162068
8. Яковів І. Інформаційно-телекомунікаційна система, концептуальна модель кіберпростору і кібербезпека. *Information Technology and Security*. 2017. Vol. 5, № 2. С. 134–144. DOI: https://doi.org/10.20535/2411-1031.2017.5.2.136981
9. Ткаченко О. Кіберпростір і кібербезпека: проблеми, перспективи, технології. *Цифрова платформа: інформаційні технології в соціокультурній сфері*. 2018. Вип. 1. С. 75–86. DOI: https://doi.org/10.31866/2617-796x.1.2018.147257
10. Дзюндзюк В. Б. Кібербезпека як один з пріоритетів національної політики. *Державне будівництво*. 2020. № 2. С.1-19. DOI: 10.34213/db.20.02.01
11. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016. URL: https://www.president.gov.ua/documents/962016-19836 (дата звернення: 14.02.2026).
12. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 14.02.2026).
13. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 № 447/2021 (рішення РНБО від 14.05.2021). URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 14.02.2026).
14. Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України : розпорядження Кабінету Міністрів України від 07.03.2025 № 204-р. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text (дата звернення: 14.02.2026).
15. Живило Є. О., Ромашко І. В. Протокол спільних дій суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти, а також при усуненні їх наслідків. *Системи управління, навігації та зв'язку*. 2024. Вип. 1. С. 66–76. DOI: 10.26906/SUNZ.2024.1.066
16. Федик В. Р., Денисенко Г. В. Теоретико-методологічні підходи до управління ризиками кібербезпеки на об'єктах критичної інфраструктури:

реагування на кіберінциденти та менеджмент кризових ситуацій. *Інформація і право*. 2024. № 1. С. 195–202. DOI: 10.37750/2616-6798.2024.1(48).300822

17. Кінзерявий В., Гнатюк В. Базові показники ефективності роботи команд реагування на кіберінциденти. *Безпека інформації*. 2014. Т. 20, № 2. С. 193–196.

18. Сахарова О. Б., Близнюк І. Л. Виявлення та реагування на кіберінциденти і кібератаки як заходи запобігання кіберзлочинності. *Наука і правоохорона*. 2023. Вип. 2. С. 220–231. DOI (Issue): https: //doi.org/10.36486/np.2023.2(60)

19. Гарасимчук О. І., Костишин Т. А., Любчик О. О., Швед М. Є. Розробка вдосконаленої методики оповіщення населення про кіберінциденти. *Інформатика та математичні методи в моделюванні*. 2025. Т. 15, № 2. С. 187–195. DOI 10.15276/imms.v15.no2.187

20. Вавіленко А. І. Процес управління кіберінцидентами як необхідний етап в організації кібербезпеки підприємства. *Інформаційна безпека людини, суспільства, держави*. 2025. № 1 (38). С. 64–71. DOI: 10.511369/2707-7276-2025-1(38)-6.

21. Саморай О. К., Семенюк О. О. Теоретичні і практичні підходи до розуміння кіберінцидентів та їхньої ідентифікації. *Європейський правничий часопис*. 2025. Вип. 8. С. 56–62. DOI: 10.36919/3041-1149(Print).8.2025.56-62.

22. Деякі питання реагування на кіберінциденти, кібератаки та кіберзагрози : Постанова Кабінету Міністрів України від 26.11.2025 № 1533. URL: https://zakon.rada.gov.ua/laws/show/1533-2025-%D0%BF#Text (дата звернення: 14.02.2026).

23. Звіт про діяльність Департаменту кіберполіції Національної поліції України у 2024 році : звіт від 31.01.2025. *Офіційний сайт Кіберполіції України.* URL: https://cyberpolice.gov.ua/news/zvit-pro-diyalnist-departamentu-kiberpolicziyi-naczionalnoyi-policziyi-ukrayiny-u--roczi-7074/ (дата звернення: 17.02.2026).

24. Фішинг, Zero Click-експлойти, AI-атаки: тенденції кіберзагроз в Україні у 2025 році. *IT Ukraine*. 07.10.2025. URL: https://itukraine.org.ua/fishing-zero-click-eksplojti-ai-ataki-tendentsiyi-kiberzagroz-v-ukrayini-u-2025-rotsi/ (дата звернення: 17.02.2026).

25. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text (дата звернення: 17.02.2026).

Information about the authors:
Spivak Maryna Viktorivna,
Doctor of Political Sciences, Professor,
Professor of the Department of Administrative Law and Process
National Academy of Internal Affairs,
1, Solomjanska Square, Kyiv, 03035, Ukraine

Dubina Oleh Mykolaiovych,
PhD, Head of the 4th division of the cybercrime counteraction
Department (in the city of Kyiv) of the
Cyberpolice Department of the National Police of Ukraine,
10, Akademika Bohomoltsia St, Kyiv, 01024, Ukraine