3. Литвиненко О. Ю. Правові новели щодо реалізації права засуджених на охорону здоров'я в місцях несвободи. *Актуальні питання юридичної науки.* 2023. № 21. С. 139.

4. Міжнародний пакт про громадянські та політичні права: Пакт ООН від 16 груд. 1966 р. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text

5. Журавська З. В. Міжнародні стандарти реалізації прав засуджених до позбавлення волі на гуманне ставлення та повагу їхньої людської гідності. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2019. Вип. 14. С. 117–125.

6. Почанська О. С. Адміністративно-правове забезпечення прав громадян, засуджених до позбавлення волі в Україні : дис. … д-ра юрид. наук : 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право»; Харківський нац. ун-т внутрішніх справ МВС України. Суми : СумДУ, 2020. 495 с.

Лашко Олександр Олександрович,
курсант ННІ № 4 Харківського національного університету внутрішніх справ
Науковий керівник:
Манжай Олександр Володимирович,
завідувач кафедри протидії кіберзлочинності ННІ № 4 Харківського національного університету внутрішніх справ, кандидат юридичних наук, професор

ПРАВОВА АРХІТЕКТОНІКА КІБЕРІМУНІТЕТУ ДЕРЖАВИ: ВІД ПАСИВНОЇ ОБОРОНИ ДО ПРОАКТИВНОЇ СТІЙКОСТІ ПУБЛІЧНОГО ПОРЯДКУ

У сучасному світі цифрова трансформація державного управління, економіки та суспільних відносин супроводжується стрімким зростанням кіберзагроз, які виходять далеко за межі технічних ризиків і набувають ознак комплексних викликів національній безпеці. Кібератаки на державні інформаційні ресурси, критичну інфраструктуру, виборчі процеси та системи публічного управління засвідчують, що традиційні підходи до забезпечення інформаційної безпеки, засновані переважно на пасивній обороні, вже не відповідають сучасним потребам захисту держави. У цих умовах особливої актуальності набуває формування нової моделі правового забезпечення

кібербезпеки, орієнтованої не лише на відбиття загроз, а й на створення стійкої, адаптивної та проактивної системи кіберімунітету держави.

Концепція кіберімунітету держави відображає якісно новий рівень розвитку правових і організаційних механізмів забезпечення кіберстійкості, де ключовим стає не реагування на вже вчинені посягання, а попередження ризиків, виявлення вразливостей і забезпечення безперервності функціонування публічних інститутів в умовах цифрових загроз. Такий підхід вимагає переосмислення правової архітектоніки кібербезпеки як системи норм, принципів, інституцій та процедур, що забезпечують захист публічного порядку в кіберпросторі. Відтак право перестає бути лише інструментом санкціонування чи регулювання окремих аспектів кіберзахисту і набуває ролі фундаментальної основи формування державної кіберстійкості.

Особливої ваги це питання набуває в умовах гібридних конфліктів, коли кіберпростір стає одним із ключових театрів протиборства, а кіберзагрози використовуються як засіб дестабілізації публічного порядку, підриву довіри до державних інституцій та порушення прав громадян. За таких обставин правова система повинна забезпечувати не лише реагування на інциденти, а й інтеграцію превентивних, координаційних та відновлювальних механізмів, спрямованих на підвищення загальної спроможності держави протистояти кібернетичним викликам. Саме тому перехід від пасивної оборони до проактивної стійкості є не лише технологічною чи управлінською трансформацією, а й передусім правовою модернізацією публічного порядку [1].

Дослідження правової архітектоніки кіберімунітету держави дозволяє виявити основні напрями вдосконалення національного законодавства, визначити оптимальні моделі взаємодії суб'єктів кібербезпеки та сформувати ефективні правові механізми забезпечення стійкості державних інституцій до кіберзагроз. У цьому контексті особливого значення набуває аналіз переходу від реактивних моделей захисту до системної проактивної стійкості, яка забезпечує збереження стабільності публічного порядку навіть в умовах постійного зростання цифрових ризиків. Саме така трансформація становить підґрунтя для побудови сучасної правової моделі кіберімунітету держави як необхідної умови гарантування її суверенітету, безпеки та ефективного функціонування в цифрову епоху.

Правова архітектоніка кіберімунітету держави є складною багаторівневою системою нормативних, інституційних та організаційних елементів, спрямованих на забезпечення стійкості держави до сучасних кіберзагроз. У науковому розумінні кіберімунітет

держави можна визначити як здатність публічних інститутів підтримувати безперервність свого функціонування, зберігати стабільність публічного порядку та гарантувати захист прав громадян навіть в умовах деструктивного впливу в кіберпросторі. Такий підхід значно ширший за традиційне розуміння кіберзахисту, яке зводилося переважно до технічного убезпечення інформаційних систем. Натомість концепція кіберімунітету акцентує увагу на поєднанні правових норм, інституційної координації та превентивного управління ризиками, що дозволяє державі діяти не лише реактивно, а й на випередження.

Формування правової основи кіберімунітету держави відбувається в межах розвитку національного законодавства у сфері кібербезпеки та інформаційної безпеки. Право в цьому контексті виконує функцію системоутворюючого механізму, оскільки саме через нормативне регулювання визначаються повноваження суб'єктів забезпечення кібербезпеки, порядок взаємодії між державними органами, правила реагування на кіберінциденти, а також гарантії дотримання прав і свобод людини в цифровому середовищі. Водночас правова архітектоніка кіберімунітету не обмежується лише регламентацією відповідальності за кіберправопорушення. Її основне завдання полягає у створенні нормативного середовища, яке забезпечує здатність держави передбачати загрози, адаптуватися до нових викликів та зберігати керованість навіть у кризових умовах.

Традиційна модель забезпечення кібербезпеки довгий час базувалася на принципах пасивної оборони. Її сутність полягала у створенні захисних механізмів для протидії зовнішнім загрозам, зокрема шляхом регламентації процедур захисту інформації, запровадження технічних засобів безпеки та встановлення юридичної відповідальності за порушення. Така модель мала значення на початкових етапах розвитку цифрових систем, однак у сучасних умовах вона демонструє обмежену ефективність. Кіберзагрози стали більш динамічними, багаторівневими та здатними завдавати шкоди не лише інформаційним ресурсам, а й функціонуванню державних інститутів загалом. У зв'язку з цим пасивна оборона, орієнтована на реагування після виникнення загрози, вже не здатна гарантувати належний рівень безпеки [2].

Перехід до моделі проактивної стійкості означає докорінну зміну правового підходу до забезпечення кібербезпеки. Проактивна стійкість передбачає формування правових механізмів, які забезпечують раннє виявлення ризиків, прогнозування загроз, резервування критичних ресурсів та підтримання безперервності діяльності органів влади в

умовах кіберінцидентів. Це означає, що держава повинна не лише створювати нормативні засоби захисту, а й забезпечувати функціонування комплексної системи правового управління кіберризиками. Така система повинна передбачати обов'язкові процедури оцінювання вразливостей державних інформаційних ресурсів, механізми координації між усіма суб'єктами кібербезпеки та правові інструменти оперативного реагування на інциденти.

Важливим елементом правової архітектоніки кіберімунітету є належне інституційне забезпечення. Ефективність державної кіберстійкості залежить від чіткого розмежування компетенції органів, відповідальних за формування та реалізацію політики у сфері кібербезпеки. У сучасних умовах до таких суб'єктів належать органи стратегічного управління, спеціалізовані служби реагування на кіберінциденти, правоохоронні структури та органи захисту критичної інфраструктури. Однак сама наявність відповідних інституцій не гарантує ефективності системи без чітко визначених механізмів взаємодії. Саме тому одним із ключових завдань правового регулювання є створення єдиної координаційної моделі, яка забезпечить оперативний обмін інформацією, узгодженість дій та безперервність управлінських процесів у разі кіберзагроз.

Особливе значення в системі кіберімунітету має правове регулювання захисту критичної інфраструктури. Саме об'єкти енергетики, транспорту, зв'язку, фінансової системи й електронного урядування є найбільш вразливими до кіберзагроз, а їх ураження може спричинити масштабну дестабілізацію публічного порядку. У зв'язку з цим правова система має передбачати спеціальні режими безпеки для таких об'єктів, включаючи підвищені вимоги до захисту інформаційних систем, процедури резервування даних, механізми аудиту та контролю за дотриманням стандартів кіберстійкості. Належне нормативне врегулювання цієї сфери дає змогу мінімізувати ризики порушення життєво важливих функцій держави та забезпечує здатність до швидкого відновлення після атак.

Окремої уваги потребує питання взаємодії держави та приватного сектору у сфері кібербезпеки. Значна частина критичної цифрової інфраструктури перебуває у володінні або користуванні приватних суб'єктів, що зумовлює необхідність нормативного закріплення їхніх обов'язків щодо забезпечення захисту інформаційних систем. Правова архітектоніка кіберімунітету має визначати правила обміну інформацією про кіберінциденти, процедури спільного

реагування на загрози та відповідальність за невиконання вимог кібербезпеки. Такий підхід забезпечує інтегрованість усіх учасників системи та підвищує загальний рівень державної кіберстійкості.

У сучасних умовах забезпечення стійкості публічного порядку в кіберпросторі стає однією з ключових функцій держави. Публічний порядок у цифровому середовищі означає такий стан функціонування суспільних відносин, за якого державні органи, громадяни та інституції можуть безперервно реалізовувати свої права й повноваження незалежно від наявності кіберзагроз. Для досягнення цього необхідно впроваджувати правові механізми, що забезпечують не лише захист від атак, а й збереження керованості системи в кризових умовах. Тому право стає не лише інструментом реагування, а й фундаментом формування стійкості держави до цифрових викликів [3].

Отже, правова архітектоніка кіберімунітету держави відображає перехід від застарілої реактивної моделі кіберзахисту до сучасної моделі проактивної стійкості. Такий перехід вимагає комплексної модернізації законодавства, удосконалення інституційних механізмів, нормативного забезпечення безперервності державного управління та інтеграції всіх суб'єктів системи кібербезпеки. Лише за умови створення цілісної правової моделі, орієнтованої на превентивність, адаптивність та відновлюваність, можливо забезпечити реальний кіберімунітет держави та гарантувати стабільність публічного порядку в умовах зростання цифрових загроз.

Список використаних джерел

1. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серп. 2021 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-39773

3. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 19 черв. 2019 р. № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п