МЕХАНІЗМ АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАХИСТУ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ В КРИЗОВИХ УМОВАХ

Богдан Олександрович МЕЛЬНИК,

аспірант Харківського національного університету внутрішніх справ

Критична інформаційна інфраструктура (КІІ) є важливим елементом забезпечення національної безпеки. У кризових умовах, таких як військові конфлікти, терористичні акти чи техногенні катастрофи, ефективний захист КІІ стає одним із першочергових завдань держави. З огляду на глобалізацію кіберзагроз та їхню еволюцію, адміністративно-правові механізми відіграють вирішальну роль у створенні надійної системи захисту.

Захист критичної інформаційної інфраструктури є ключовим елементом забезпечення національної безпеки, який охоплює широкий спектр організаційних, технічних і правових заходів. У сучасних умовах, коли інформаційні технології стали основою функціонування більшості галузей, надійний захист таких об’єктів набуває особливого значення. До критичної інформаційної інфраструктури належать об’єкти, від функціонування яких залежить стабільність економіки, енергетичної сфери, транспорту, зв’язку, систем охорони здоров’я та інших важливих секторів держави. Це визначено як на національному рівні, зокрема в Законі України "Про основні засади забезпечення кібербезпеки України", так і в міжнародних нормативних актах. У кризових умовах, які можуть включати військові дії, терористичні загрози чи техногенні катастрофи, загрози для критичної інформаційної інфраструктури значно зростають. Серед ключових викликів виділяють кібератаки, втручання в системи управління, а також фізичні загрози для об'єктів, які забезпечують інформаційну безпеку. У таких умовах адміністративно-правові механізми захисту стають інструментом першої необхідності. Вони включають регламентацію діяльності суб’єктів, які забезпечують функціонування критичної інформаційної інфраструктури, а також координацію дій між органами державної влади та приватним сектором.

Нормативно-правове регулювання є основою для ефективного захисту критичних об'єктів. Впровадження відповідних законодавчих актів, які визначають порядок функціонування, контроль та відповідальність у цій сфері, дозволяє створити міцний правовий фундамент для забезпечення кібербезпеки. Зокрема, в Україні це включає визначення обов'язків власників та операторів критичної інформаційної інфраструктури, встановлення вимог до технічного захисту даних, а також впровадження заходів для попередження, виявлення та реагування на інциденти. Важливою складовою адміністративно-правового захисту є контроль і нагляд з боку уповноважених державних органів. Це забезпечує дотримання суб’єктами господарювання встановлених норм і стандартів. Зокрема, Державна служба спеціального зв’язку та захисту інформації України виконує функції моні-

торингу, аналізу та забезпечення кіберзахисту, впроваджуючи сучасні технологічні рішення. Окрім цього, органи виконавчої влади розробляють нормативно-правові акти, спрямовані на удосконалення захисту об'єктів критичної інформаційної інфраструктури, а також здійснюють навчання та тренінги для суб'єктів, що забезпечують їхню роботу. Міжнародна співпраця в цій сфері також є невід'ємною складовою ефективного захисту. Обмін досвідом, використання кращих світових практик і впровадження міжнародних стандартів дозволяють забезпечити високий рівень безпеки. Україна активно співпрацює з міжнародними організаціями, такими як НАТО, ЄС та ООН, що сприяє адаптації найновіших методик і технологій для захисту критичної інформаційної інфраструктури.

Таким чином, теоретико-правові засади захисту критичної інформаційної інфраструктури базуються на поєднанні нормативно-правового регулювання, адміністративного контролю, сучасних технологічних рішень і міжнародної співпраці. Ця комплексність є ключовою для створення ефективної системи захисту, здатної адаптуватися до змінних умов і забезпечувати безпеку критичних об'єктів навіть у найскладніших кризових ситуаціях.

Особливості реалізації адміністративно-правових механізмів захисту критичної інформаційної інфраструктури в кризових умовах полягають у швидкій адаптації до нових загроз та умов, що виникають через зовнішні чи внутрішні фактори. Кризові ситуації, як-от військові конфлікти, природні катаклізми чи масові кібератаки, вимагають негайного реагування для запобігання масштабним наслідкам. У таких обставинах держава повинна діяти за допомогою спеціально створених механізмів, спрямованих на забезпечення безперервного функціонування критичної інформаційної інфраструктури. В умовах кризи першочергову роль відіграють спеціалізовані органи, створені для моніторингу та нейтралізації кіберзагроз. В Україні таким органом є CERT-UA, який виконує функції виявлення, аналізу та запобігання кібератакам. Активізація його роботи в критичних ситуаціях дозволяє швидко ідентифікувати загрози, зокрема ті, що спрямовані на об'єкти енергетики, транспорту чи фінансової інфраструктури. Окрім оперативного реагування, організація також розробляє рекомендації для суб'єктів критичної інформаційної інфраструктури, що сприяє підвищенню їхньої готовності до можливих інцидентів. Кризові умови передбачають застосування спеціальних адміністративних процедур, які впроваджуються через рішення уряду або відповідних органів виконавчої влади. Такі заходи можуть включати обов'язкові перевірки систем захисту, введення тимчасових обмежень доступу до певних ресурсів або вимогу підвищення рівня захисту інформаційних систем. Ці процедури розробляються з урахуванням специфіки кризової ситуації, що забезпечує їхню ефективність. Наприклад, під час загострення військових дій можуть бути запроваджені додаткові перевірки каналів комунікації, аби уникнути витоку критично важливої інформації. Одним із ключових аспектів у кризових умовах є налагодження інформаційної взаємодії між державними структурами, приватними суб'єктами критичної інфраструктури та міжнародними партнерами. Обмін інформацією про можливі загрози та вразливості дозволяє своєчасно

запобігти значним збиткам. Інтеграція України у глобальну систему кібербезпеки сприяє отриманню передових інструментів і технологій, що допомагають мінімізувати наслідки кризових подій. Посилення адміністративної відповідальності за порушення встановлених норм і стандартів у сфері захисту критичної інформаційної інфраструктури є важливим елементом у кризовий період. Штрафи, призупинення діяльності або інші санкції стимулюють суб'єктів господарювання дотримуватися нормативних вимог. В умовах кризи такі заходи дозволяють підтримувати належний рівень кіберзахисту навіть у складних умовах. Для підвищення готовності адміністративних структур і суб'єктів критичної інфраструктури до дій у кризових ситуаціях необхідно регулярно проводити тренування та симуляції. Такі заходи дозволяють перевірити ефективність існуючих механізмів захисту, виявити слабкі місця та вдосконалити процес реагування. На практиці це реалізується через моделювання різних сценаріїв криз, включаючи масові кібератаки, фізичні загрози чи комбіновані інциденти, що ускладнюють захист об'єктів.

Ми вважаємо, що у кризових умовах головним завданням держави залишається забезпечення безперебійного функціонування критичної інформаційної інфраструктури. Це можливо лише за умови застосування ефективних адміністративно-правових механізмів, які враховують специфіку та масштаби кожної окремої кризи.

Підсумовуючи вище викладене можемо зробити висновок, що у кризових умовах захист критичної інформаційної інфраструктури є пріоритетним завданням для держави. Ефективність адміністративно-правових механізмів залежить від їхньої адаптивності, оперативності та комплексності. Важливим є не лише створення нормативно-правової бази, але й її дієве впровадження, що передбачає належний адміністративний контроль, посилення відповідальності за порушення та розширення міжнародного співробітництва. Удосконалення механізмів адміністративно-правового захисту КІІ потребує системного підходу, включаючи впровадження новітніх технологій, підвищення кваліфікації персоналу та забезпечення координації між усіма суб'єктами процесу. Лише за таких умов можна гарантувати належний рівень захищеності КІІ в умовах криз та загроз.