

Андрій СОБАКАРЬ
професор кафедри
адміністративно-правових дисциплін
та публічного управління
Дніпровського державного
університету внутрішніх справ
(м. Дніпро, Україна),
доктор юридичних наук, професор

ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ ЯК СКЛАДОВА СИСТЕМИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЕРЖАВИ

У сучасних умовах цифровізації суспільства критична інформаційна інфраструктура перетворюється на системоутворюючий елемент державності, що забезпечує функціонування ключових секторів національної інфраструктури та ефективність державного управління.

Її безперебійна робота є не лише технічною передумовою стабільності, а й політичним фактором легітимності влади, оскільки саме через інформаційні та телекомунікаційні системи здійснюється координація діяльності енергетичного, фінансово-банківського, транспортного, оборонного та інших стратегічних секторів.

Порушення функціонування критичної інформаційної інфраструктури здатне спричинити масштабні соціально-економічні збої, параліч систем життєзабезпечення країни, втрату контролю з боку органів державного управління, що у сукупності формує передумови політичної дестабілізації.

У системі національної безпеки України базовим нормативно-правовим актом, що визначає засади функціонування державної політики у сфері кіберзахисту, є Закон України «Про основні засади забезпечення кібербезпеки України», у якому закріплено понятійний апарат (кіберзагроза, кібератака, кіберінцидент, кіберзахист, критична інформаційна інфраструктура тощо), визначено об’єкти кібербезпеки та кіберзахисту, а також встановлено систему суб’єктів, відповідальних за формування та реалізацію державної політики у зазначеній сфері. Нормативна конструкція Закону базується на принципах верховенства права, пропорційності, пріоритетності запобіжних заходів, державно-приватної взаємодії та міжнародного співробітництва, що відповідає сучасним стандартам ЄС і НАТО. Особливого значення у контексті забезпечення стійкості критичної інформаційної інфраструктури набувають положення щодо функціонування національної системи кібербезпеки, координаційної ролі Ради національної безпеки і оборони України, діяльності Національного координаційного центру кібербезпеки, а також створення підрозділів з кіберзахисту та запровадження системи реагування на кіберінциденти. Названий документ формує комплексну модель протидії кіберзагрозам, що поєднує правові, організаційні та технічні механізми захисту, визначає обов’язки операторів критичної інфраструктури та передбачає інструменти активної протидії агресії у кіберпросторі, що є ключовим елементом зміцнення національної безпеки України в умовах воєнного стану [1].

Результативність сучасних технологій і систем виявлення кіберзагроз значною мірою визначається своєчасністю отримання та надійністю аналітичних даних про активність зловмисників ще на ранніх етапах підготовки та здійснення атак на інформаційні ресурси, зокрема об’єкти критичної інфраструктури. Узагальнення міжнародної практики свідчить, що найбільш перспективним напрямом розроблення інтелектуальних систем моніторингу є впровадження ієрархічних багаторівневих моделей, здатних забезпечити поетапне розпізнавання кіберзагроз на початкових стадіях їх реалізації. Такий підхід дозволяє структурувати процес захисту розподілених критично важливих інформаційних систем як комплекс взаємопов’язаних локальних завдань, інтегрованих у єдину координовану систему управління безпекою [2, с. 18].

Загрози безпеці критичної інформаційної інфраструктури у науковій літературі розглядаються як складова загроз кібернетичній безпеці та можуть мати як умисний, так і неумисний характер. Йдеться про можливість здійснення так званої «екзистенційної кібератаки», яка здатна завдати системного, життєво небезпечного удару по інфраструктурі держави.

До основних джерел загроз кібернетичній безпеці, зокрема об’єктам критичної

інформаційної інфраструктури, належать різні категорії суб'єктів, діяльність яких відбувається у кіберпросторі. Передусім ідеться про іноземні розвідувальні структури, які можуть здійснювати кібероперації з метою отримання стратегічної інформації, дестабілізації або навіть руйнування інформаційної інфраструктури іншої держави. Вагомим чинником ризику залишаються організовані злочинні угруповання, що використовують цифрові технології для незаконного збагачення, а також окремі хакери, які застосовують шкідливе програмне забезпечення для несанкціонованого втручання в роботу мережевих ресурсів.

Окрему категорію становлять хактивісти, котрі здійснюють кібератаки з ідеологічних або політичних мотивів, спрямовуючи їх проти державних чи публічних інформаційних ресурсів. Підвищену небезпеку також становлять інсайдери – особи, що мають легальний доступ до внутрішніх мереж організацій та можуть використовувати його всупереч інтересам установи. Крім того, серйозною загрозою виступають терористичні групи, які здатні застосовувати кіберінструменти для блокування або знищення елементів критичної інфраструктури з метою завдання шкоди державі та суспільству.

З огляду на характер їх діяльності, умисні загрози найчастіше пов'язані з діями іноземних спецслужб і терористичних організацій, тоді як окремі кібератаки з боку злочинних груп, хакерів чи інсайдерів можуть мати як свідомий, так і ситуативний або опосередкований характер.

Взаємозв'язок між безпекою критичної інформаційної інфраструктури та політичною стабільністю виявляється через механізми соціально-політичної дестабілізації, які передбачають переведення суспільства у стан кризової нестійкості шляхом цілеспрямованого впливу на його інфраструктурні вразливості. Параліч або руйнування об'єктів критичної інфраструктури може слугувати каталізатором посилення соціального невдоволення та делегітимації влади. У цьому контексті атаки на критичну інформаційну інфраструктуру виступають інструментом асиметричного тиску, що дозволяє досягати політичних цілей без прямої військової агресії. Деструктивний вплив на інфраструктуру здатний створювати штучні соціально-економічні кризи, провокувати масові протести та підштовхувати політичну систему до критичних точок розвитку.

Особливого значення набуває феномен цифрового активізму, який трансформується із засобу комунікації громадянського суспільства у потенційний інструмент політичного впливу в кіберпросторі. Використання соціальних мереж, онлайн-платформ та інформаційних технологій поєднується із застосуванням кібератак, DDoS-операцій та втручання у функціонування державних інформаційних ресурсів. У межах цього явища формується концепція «цифрового спротивлення», яка передбачає синергію офлайн-протестів та кібернетичних дій, спрямованих на порушення роботи систем державного управління та критичної інфраструктури. Хоча така модель дестабілізації не була реалізована у завершеному вигляді, окремі її елементи простежуються у практиках сучасних політичних криз.

Отже, критична інформаційна інфраструктура виступає не лише технологічною основою функціонування держави, а й стратегічним ресурсом національної безпеки, руйнування якого може стати тригером системної політичної кризи. Забезпечення її стійкості вимагає комплексного підходу, що поєднує правові, організаційні та технологічні механізми захисту. У контексті сучасних гібридних загроз питання безпеки критичної інформаційної інфраструктури набуває ключового значення для збереження суверенітету, стабільності політичних інститутів та запобігання дестабілізаційним сценаріям у кіберпросторі.

---

1. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року. Відомості Верховної Ради України. 2017. № 45. Ст. 403.

2. Діордіца І.В. Класифікація кіберзагроз та їх легітимація у нормативно-правових актах України URL: https://goal-int.org/klasifikatsiya-kiberzagroz-ta-yih-legitimatsiya-u-normativno-pravovih-aktah-ukrayini/.