Гапєєва О. М.
доктор економічних наук, професор,
професор кафедри економіки та менеджменту,
Навоїйський державний гірничо-технологічний університет
м. Навої, Узбекистан;
професор кафедри економіки та економічної безпеки,
Університет митної справи та фінансів
м. Дніпро, Україна
Ромашко С. М.
аспірант кафедри економіки та економічної безпеки,
Університет митної справи та фінансів
м. Дніпро, Україна

DOI: https://doi.org/10.36059/978-966-397-611-2-4

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК КОМПОНЕНТ НАЦІОНАЛЬНОЇ СТІЙКОСТІ: БАГАТОРІВНЕВА МОДЕЛЬ УПРАВЛІННЯ ТА МОНІТОРИНГ ЗАГРОЗ

Під час гібридної війни інформаційна сфера стала одним із ключових театрів протистояння. Зростання кібератак, дезінформації та психологічних операцій підриває довіру до інституцій і погіршує функціонування держави. Для збереження національної безпеки необхідно розглядати інформаційну безпеку як невід'ємну складову національної стійкості. Згідно з Концепцією національної системи стійкості [1; 4], стійкість – це здатність держави та суспільства ефективно протистояти загрозам, адаптуватися до змін і підтримувати стале функціонування. Інформаційна безпека, за сучасними дослідженнями, є не просто технічним елементом, а фундаментальним чинником формування стійкості: вона охоплює здатність суспільства адаптуватися, чинити спротив та зберігати цілісність перед складними інформаційними загрозами [2]. Проте в Україні досі відсутня цілісна концепція управління інформаційною безпекою на різних рівнях та узгоджена система індикаторів її моніторингу.

Національна стійкість означає здатність держави й суспільства протистояти загрозам будь-якого походження, адаптуватися до мінливого безпекового середовища й підтримувати сталість функціонування. Спираючись на роботу [3], цей процес забезпечується

сукупністю базових критеріїв: надійність (fault tolerance), надлишковість ресурсів, адаптивність, здатність поглинати удари (shock absorption) тощо. Функціональні критерії – готовність до реагування, швидкість реакції, ефективність реагування та швидкість відновлення – оцінюються через відповідні показники (наприклад, час на відновлення системи, ступінь дублювання ресурсів) [5].

Інформаційна безпека охоплює захист інформаційних ресурсів (дані, мережі, служби) від загроз (кібератак, кібершпигунства, дезінформації тощо). В умовах інформаційної війни вона забезпечує критичні засоби психологічної стійкості суспільства. Як зазначає [2], інформаційна безпека – це комплексне явище (законодавчі, стратегічні, технічні, освітні, соціальні заходи), яке інтегрується в систему національної стійкості нарівні з політичним та економічним компонентами. Іншими словами, успіх у протидії інформаційним загрозам прямо впливає на здатність держави швидко відновлювати свою життєдіяльність після криз.

Основна ідея багаторівневої моделі – розподіл повноважень та відповідальності за інформаційну безпеку на різні рівні влади. Концепція [1] підкреслює, що багато- чи багаторівнева структура дозволяє будувати спроможності на державному, регіональному та місцевому рівнях. У запропонованій моделі виділено:

– Державний рівень: стратегічне планування, затвердження загальних політик і законодавчих ініціатив (офіс Президента, РНБО, Кабмін).

– Секторальний рівень: спеціалізовані відомства (Мінцифри, Держспецзв’язку, СБУ, НБУ тощо) – розробка галузевих стандартів, проведення аудитів, технічний захист, координація міжвідомчих програм.

– Регіональний рівень: облдержадміністрації, обласні центри реагування – адаптація загальнодержавних політик до місцевих умов, моніторинг ситуації, інформування федеральних органів.

– Місцевий рівень: органи місцевого самоврядування та громади – захист локальної інфраструктури, виконання превентивних та просвітницьких заходів, інформування громадян.

Важливо, що між рівнями встановлено зворотний зв'язок: інформація про загрози та інциденти надходить знизу вгору, а управлінські рішення і стандарти – зверху вниз. Це забезпечує горизонтальну та вертикальну синхронізацію зусиль і створює адаптивну, інтегровану структуру, здатну гнучко реагувати на нові

виклики. Рівні зв’язані каналами стратегічного керування, обміну розвідувальними даними та зворотного зв’язку (рис. 1).

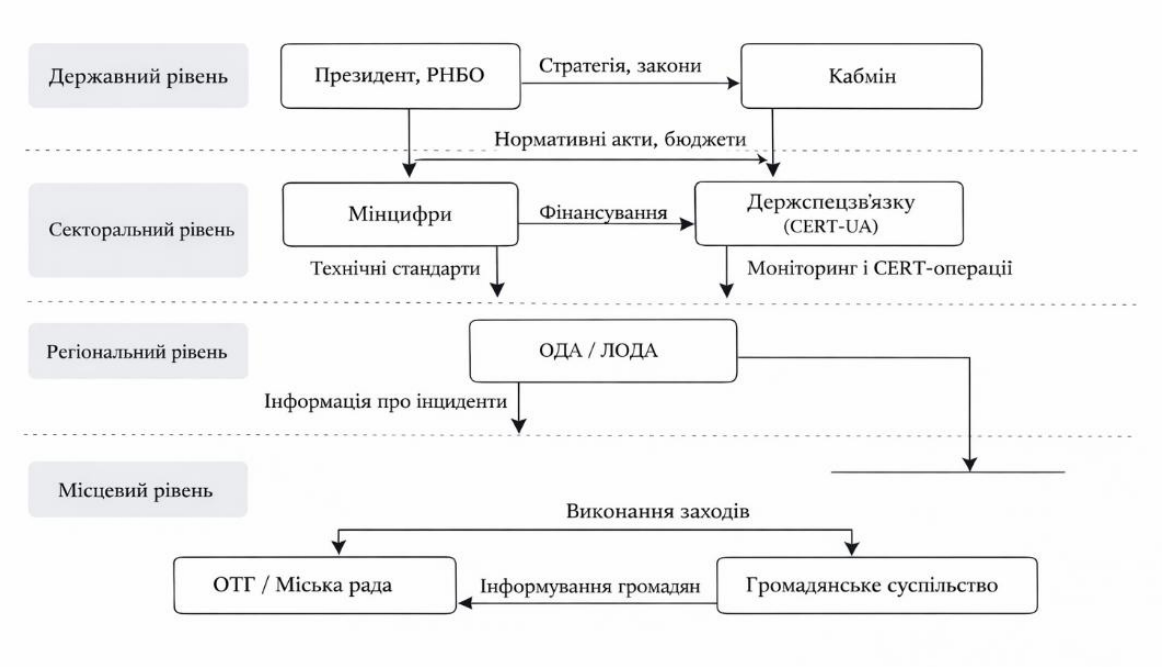

Рис. 1. Багаторівнева модель управління інформаційною безпекою

Джерело: сформовано автором

На підставі проведених досліджень можна визначити основні напрями забезпечення національної стійкості що базуються на побудові багаторівневої моделі управління та моніторинг загроз:

Удосконалення законодавства: Прийняти комплексний закон про кібербезпеку та інформаційну безпеку з чітким розподілом повноважень; виділити бюджетне фінансування ІБ-програм (не менше 10 % від загального бюджету безпеки).

Зміцнення координації: Створити міжвідомчий центр (координаційну раду) з інформаційної безпеки за участі РНБО, силових структур і Мінцифри; проводити регулярні тренінги та симуляції кібератак.

Кіберзахист інфраструктури: Впровадити резервні канали зв’язку для критичних систем, розгорнути системи швидкого відновлення даних, застосувати сучасні технології виявлення загроз (штучний інтелект, IDS/IPS).

Підвищення обізнаності населення: Інвестувати в кіберосвіту у школах і університетах; проводити інформаційні кампанії та тренінги з кібергігієни та критичного мислення щодо інформації.

Міжнародна співпраця: Активізувати обмін інформацією про кіберзагрози з партнерами (ЄС, НАТО, міжнародні CERT-форуми); адаптувати досвід побудови центрів аналізу загроз і оцінки ризиків.

Інформаційна безпека повинна стати невід'ємною частиною державної політики нац. стійкості. Запропонована багаторівнева модель та система моніторингу інтегрують зусилля різних відомств і суспільства у єдину систему превенції та реагування. Як підкреслює [2], інформаційна безпека – це комплексне явище, інтегроване в систему стійкості на рівні з політичними та економічними компонентами. Для реалізації цього підходу потрібні пріоритетні інвестиції у кіберзахист, чітке законодавче врегулювання відповідальності та тісна міжвідомча координація. Лише за таких умов інформаційна безпека ефективно посилить стійкість держави і забезпечить сталу роботу її критичних систем навіть у кризові моменти.

Література:

1. Про рішення Ради національної безпеки і оборони України від 20 серпня 2021 року «Про запровадження національної системи стійкості» : Указ Президента України від 27 вересня 2021 р. № 479/2021. URL: https://zakon.rada.gov.ua/laws/show/479/2021 (дата звернення: 06.03.2026).
2. Ульяненко К. В. Інформаційна безпека як фактор формування національної стійкості України. *Політикус : науковий журнал*. 2025. № 2. DOI: https://doi.org/10.24195/2414-9616.2025-2.2.
3. Резнікова О.О. Національна стійкість в умовах мінливого безпекового середовища : монографія. Київ : НІСД, 2022. С. 456.
4. Грибіненко О.М. Міжнародна економічна безпека в контексті сталого розвитку: монографія. Дніпро: Середняк Т.К., 2020. С. 432.
5. Ромашко С.М. Концептуальна модель управління інформаційною безпекою в системі національної безпеки України. *Національні інтереси України*. 2025. №12 (17). С.1163–1177. DOI: https://doi.org/10.52058/3041-1793-2025-12(17)-1163-1177