СЛУЖБА БЕЗПЕКИ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ
НАВЧАЛЬНО-НАУКОВИЙ ТРЕНІНГОВИЙ ЦЕНТР
ОПЕРАТИВНО-БОЙОВОЇ ПІДГОТОВКИ

ОПЕРАТИВНО-БОЙОВА ДІЯЛЬНІСТЬ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ В УМОВАХ ВОЄННОГО СТАНУ

Матеріали Всеукраїнської науково-практичної конференції

ВИПУСК 2

Київ
2025

УДК 351.86(06)
О-60

Рекомендовано до друку навчально-науковим тренінговим центром оперативно-бойової підготовки (протокол № 10 від 13 листопада 2025 року)

Оперативно-бойова діяльність сил сектору безпеки і оборони
О-60 в умовах воєнного стану : матеріали Всеукраїнської науково-практичної конференції (м. Київ, 30 жовт. 2025 р.). Київ : НА СБУ, 2025. Вип. 2. 257 с.

До збірника увійшли матеріали Всеукраїнської науково-практичної конференції представників сектору безпеки і оборони України, наукових та науково-педагогічних працівників, здобувачів освіти та інших зацікавлених осіб. На науковому заході розглядались такі напрямки: підготовка кадрів для потреб сил сектору безпеки і оборони в сучасних умовах; міжвідомча взаємодія у рамках реалізації заходів із забезпечення національної безпеки і оборони; безпека та захист об’єктів національної критичної інфраструктури; досвід бойового застосування сил оборони при відсічі збройної агресії рф; питання психологічного забезпечення військовослужбовців при виконанні оперативно-бойових завдань в районі проведення бойових дій; застосування стратегічних комунікацій у діяльності сил сектору безпеки і оборони (цивільно-військове співробітництво, інформаційні та психологічні операції); особливості організації спеціальної фізичної підготовки військових формувань та правоохоронних органів; застосування роботизованих систем при виконанні оперативно-бойових завдань та інші питання, пов’язані з напрямами науково-практичної конференції.

Збірник матеріалів буде корисним для здобувачів вищої освіти, аспірантів, наукових співробітників, співробітників сил безпеки і оборони України.

Автори несуть повну відповідальність за підбір, точність наведених фактів, цитат, галузевої термінології, власних імен та інших відомостей.

УДК 351.86(06)

ЗМІСТ

ВІТАЛЬНЕ СЛОВО

ВИСТУПИ УЧАСНИКІВ МІЖВІДОМЧОГО КРУГЛОГО СТОЛУ

1 ПІДГОТОВКА КАДРІВ ДЛЯ ПОТРЕБ СИЛ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ В СУЧАСНИХ УМОВАХ

2 МІЖВІДОМЧА ВЗАЄМОДІЯ У РАМКАХ РЕАЛІЗАЦІЇ ЗАХОДІВ ІЗ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ І ОБОРОНИ

ПОМАЗА-ПОНОМАРЕНКО А. Л.,
доктор наук з державного управління, професор,
завідувач науково-дослідної лабораторії
з дослідження проблем управління
у сфері цивільного захисту,
Національний університет
цивільного захисту України

ТАРАДУДА Д. В.,
кандидат технічних наук, доцент,
професор кафедри управління діяльністю
підрозділів цивільного захисту інституту
післядипломної освіти,
Львівський державний університет
безпеки життєдіяльності

ЗАБЕЗПЕЧЕННЯ СТІЙКОСТІ ФУНКЦІОНУВАННЯ ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стійкість функціонування об'єктів критичної інфраструктури (КІ) є визначальною умовою національної безпеки, економічної стабільності та життєдіяльності суспільства. В умовах воєнного стану, масштабних гібридних загроз, кібератак та терористичних ризиків, питання забезпечення безперервності роботи критичної інфраструктури (далі – КІ) стає одним із головних напрямів державної політики безпеки. Для України, яка зазнала руйнувань енергетичної, транспортної, комунікаційної інфраструктури внаслідок воєнних дій, формування системи стійкості КІ означає не лише відновлення, а й створення нової архітектури безпеки, заснованої на принципах адаптивності, цифрової інтегрованості та взаємодії секторів.

У науковій літературі поняття resilience (стійкість, життєздатність) розглядається як здатність системи передбачати, поглинати, адаптуватися та швидко відновлюватися після деструктивних впливів. Стійкість критичної інфраструктури включає три основні рівні:

1. Технічна стійкість – здатність інженерних систем зберігати функціональність у разі фізичного чи кібернетичного ураження.
2. Організаційна стійкість – ефективність управління кризами, координація суб'єктів безпеки.
3. Соціальна стійкість – готовність населення та персоналу до дій у надзвичайних ситуаціях.

Методологічно концепція стійкості КІ [1] базується на моделі адаптивного управління (adaptive management), ризик-орієнтований підхід, а також принципи управління безперервністю бізнесу (Business Continuity Management).

Державна політика України у сфері забезпечення стійкості КІ регулюється низкою документів, а саме: Закон України «Про критичну

інфраструктуру», що визначає правові основи функціонування, захисту та відновлення КІ; Постанова КМУ «Про затвердження Порядку формування переліку об'єктів критичної інфраструктури»; Стратегія забезпечення кібербезпеки України (на 2021–2025 роки); Стратегія національної безпеки України (2020 р.), що закріплює принципи захисту КІ як складової безпекової політики [2]. Однак практична реалізація цих документів стикається з такими проблемами: відсутністю інтегрованої інформаційної системи моніторингу стану КІ, фрагментарністю управлінських повноважень й обмеженими ресурсами для модернізації об'єктів.

Серед основних проблем забезпечення стійкості КІ можна виокремити такі:

1. Високий рівень фізичних загроз – цілеспрямовані обстріли енергетичних, транспортних, об'єктів ЖКГ та ін. під час війни.

2. Кібератаки на енергетичні системи (наприклад, атака на «Укренерго» (грудень 2022 р.), коли відбулася спроба порушити енергопостачання через шкідливе ПЗ.

3. Нестача резервних потужностей і децентралізованих елементів інфраструктури.

4. Недостатній рівень міжвідомчої координації через інституційне дублювання функцій (між Міноборони, НКЦК при РНБО, Держспецзв'язку та Міненерго, СБУ, ДСНС тощо).

5. Відсутність системи аудиту стійкості (відсутні стандарти оцінки ризиків для об'єктів різних секторів КІ (енергетичного, транспортного, ІТ).

6. Залежність від імпортних технологій у галузях енергетики, зв'язку, хімічної промисловості, що ускладнює самостійне відновлення після руйнувань.

Щодо ключових напрямів державної політики щодо забезпечення стійкості КІ, то серед них можна визначити такі:

1. Розвиток системи оцінки ризиків на об'єктах КІ. Упровадження інтегрованої системи Risk Assessment & Management System для всіх секторів КІ, що забезпечує прогнозування наслідків і сценарне моделювання криз.

2. Забезпечення кіберстійклості КІ, що передбачає розгортання національної мережі центрів реагування на кіберінциденти (CERT-UA, SOC у відомствах), а також створення системи сертифікації ІТ-продуктів, що використовуються на об'єктах КІ.

3. Розвиток локальних енергетичних систем, мікромереж, відновлюваних джерел енергії, які підвищують автономність об'єктів КІ у кризових ситуаціях.

4. Підвищення результативності інституціональної взаємодії шляхом упровадження моделі мережевого врядування (network governance), що поєднує державні, приватні та громадські структури у спільному забезпеченні безпеки КІ.

5. Забезпечення накопичення та повноцінної реалізації людського капіталу. Це вимагає оперативного навчання необхідних кадрів з управління кризами та безперервності діяльності, підвищення кваліфікації персоналу КІ у сфері безпеки, кіберзахисту та протидії гібридним загрозам.

Європейський Союз у межах Директиви (EU) 2022/2557 про стійкість критичних суб'єктів запровадив принцип «all-hazards approach», що передбачає застосування комплексного підходу до управління всіма типами ризиків. США реалізують концепцію Critical Infrastructure Security and Resilience (CISR), що передбачає тісну співпрацю між державою та приватним сектором через Агентство з кібербезпеки та безпеки інфраструктури (CISA). Ізраїль формує багаторівневу модель захисту з інтеграцією елементів цивільної оборони, кіберзахисту і локальної самоврядності [4; 5].

Для України адаптація таких практик може базуватися на створенні Національної ради з питань стійкості КІ при РНБО, а також публічно-приватного партнерства у сфері модернізації критичної інфраструктури. У цьому контексті доцільно розглянути технологічні аспекти стійкості КІ, що забезпечується за рахунок: 1) систем моніторингу і раннього виявлення інцидентів (Early Warning Systems); 2) резервного копіювання і дублювання критичних елементів (redundancy & backup); 3) технології штучного інтелекту для прогнозування пошкоджень; 4) інтернет речей (IoT) у системах управління ресурсами; 5) блокчейн-технологій для забезпечення цілісності критичних даних.

Важливим компонентом стійкості КІ є готовність населення до кризових ситуацій, формування культури безпеки, довіри до державних інститутів, ефективна інформаційна політика, що запобігає панічним настроям під час криз.

Отже, стійкість критичної інфраструктури – це не лише технічне завдання, а системна державна стратегія, що охоплює правові, інституційні, кадрові, технологічні та соціальні компоненти. Її забезпечення можливе лише за умов інтеграції принципів resilience governance у політику національної безпеки, розбудови міжсекторної співпраці, переходу від реактивного до проактивного управління ризиками, залучення громадянського суспільства до моніторингу та контролю у сфері безпеки КІ. Стійкість критичної інфраструктури – це стратегічний ресурс держави, що визначає її здатність не лише виживати, а й розвиватися в умовах багатовимірних криз.

Список використаних джерел:

1. Лазор О. Я., Юник І. Г., Чемерпільська А. М. Організаційно-правові засади забезпечення кібернетичної безпеки об'єктів критичної інформаційної інфраструктури України: формування та розвиток // Державне управління: удосконалення та розвиток. 2024. № 5. URL: https://www.nayka.com.ua/index.php/dy/article/view/3677/3712.

2. Офіційний веб-сайт Верховної Ради України. URL: https://zakon.rada.gov.ua/laws/show/1030-2022-%D0%BF#Text.
3. Помаза-Пономаренко А. Л., Тарадуда Д. В. Застосування цифрових технологій у сфері критичної інфраструктури для забезпечення цивільної безпеки // Матеріали Науково-практичної конференції «Інноваційні підходи до розвитку технологій та економіки» (27.06.2024 р., м. Свалява). 2024. С. 248–251.
4. Помаза-Пономаренко А. Л., Тарадуда Д. В. Механізми забезпечення цивільної безпеки України: аспекти попередження НС на об'єктах військово-промислового комплексу // Публічне адміністрування та національна безпека. 2024. № 3 (44). URL: https://www.inter-nauka.com/issues/administration2024/3/9732.
5. Pomaza-Ponomarenko A., Taraduda D., Leonenko N., Poroka S., Sukhachov M. Ensuring the safety of citizens in times of war: aspects of the organization of civil defense // AD ALTA: Journal of Interdisciplinary Research. 2024. Vol. 14. Issue 1. Pp. 216–220.

РЕМІННИЙ О. В.,
курсант, Національний університет
цивільного захисту України

БОРСУК О. В.,
кандидат технічних наук,
викладач кафедри,
Навчально-науковий інститут пожежної
та техногенної безпеки
Національного університету
цивільного захисту України

ВПЛИВ БОЙОВИХ ДІЙ НА СТІЙКІСТЬ ЕНЕРГЕТИЧНИХ СИСТЕМ ТА ВИНИКНЕННЯ АВАРІЙНИХ РЕЖИМІВ КОРОТКОГО ЗАМИКАННЯ

Об'єкти енергетики є пріоритетними цілями під час воєнної агресії рф, адже їх ураження призводить до масштабних порушень у роботі енергосистеми, відключення електропостачання об'єктів критичної та цивільної інфраструктури. Руйнування підстанцій, ліній електропередач і трансформаторів безпосередньо впливає на стійкість електромережі та створює умови для виникнення аварійних режимів, найпоширенішими з яких є короткі замикання [1].

Ударні хвилі вибухів і прямі обстріли можуть пошкоджувати ізоляцію та контакти обладнання, порушувати цілісність обмоток трансформаторів, що призводить до електричних пробоїв і коротких замикань. Такі аварії здатні спричинити відключення великих ділянок мережі та порушити безперебійне електропостачання [1].

Пошкодження енергетичних об'єктів можна класифікувати як: **прямі** – фізичне руйнування унаслідок обстрілів чи вибухів і **побічні або вторинні** – пошкодження, що виникають через аварійні режимів та нестабільність електричних систем, що сприяють підвищенню