2. Створення енергетичного резерву: формування стратегічних запасів газу (на рівні 20 млрд куб. м) та вугілля для забезпечення автономності в кризових ситуаціях;

3. Децентралізацію енергосистеми: розвиток локальних енергетичних мереж і мікрогрідів для зниження вразливості до атак і аварій;

4. Інвестиції в інновації: розробку технологій зберігання енергії (батареї, водневі системи) для підтримки ВДЕ та стабільності мережі;

5. Посилення кіберзахисту: впровадження систем моніторингу та захисту енергетичної інфраструктури від кібератак.

Енергетична безпека України є критично важливою для її національної стійкості, особливо в умовах війни та геополітичних викликів. Основні ризики – залежність від імпорту, вразливість інфраструктури та застарілість обладнання – вимагають комплексного підходу до управління, який включає диверсифікацію джерел, модернізацію та розвиток ВДЕ. Попри досягнення, такі як інтеграція до ENTSO-E та зниження газової залежності, прогрес у реалізації стратегічних цілей залишається обмеженим через фінансові й організаційні бар'єри. Стратегічне планування має зосередитися на довгостроковій трансформації енергосектора, підвищенні енергоефективності та залученні міжнародної підтримки. Подальші дослідження повинні охоплювати моделювання сценаріїв енергетичних криз і оцінку економічної доцільності переходу до «зеленої» енергетики.

Володимир МИРОШНИЧЕНКО
аспірант кафедри
соціально-економічних дисциплін
Дніпровського державного
університету внутрішніх справ
https://orcid.org/0009-0004-0217-0940

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ В КОНТЕКСТІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

Сучасний світ неможливо уявити без інформаційних технологій, які проникають у всі сфери життя – від економіки до освіти. Інтеграція глобалізаційних процесів у демократичне суспільство характеризується стрімким розвитком інформаційних технологій, які відіграють ключову роль у забезпеченні національної безпеки. В умовах глобалізації та зростаючих кіберзагроз країни змушені адаптувати свої стратегії безпеки, враховуючи вплив цифрових технологій на різні сфери життя.

Інформаційні технології стали ключовим інструментом у забезпеченні національної безпеки. Вони використовуються в оборонній сфері, системах управління державою, правоохоронних органах і навіть у соціальних мережах, де формується суспільна думка. Завдяки цифровим технологіям держави можуть ефективніше захищати свої кордони, здійснювати моніторинг кіберзагроз і забезпечувати безпеку громадян [1].

Інформаційні технології охоплюють широкий спектр аспектів, що безпосередньо впливають на безпеку держави. Серед них варто виділити:

– кібербезпека та захист критичної інфраструктури;

– інформаційна війна та гібридні загрози;

– захист персональних даних тощо.

Інформаційні системи державних установ, банків, енергетичних компаній, транспортних мереж є потенційними цілями кібератак. Захист цих систем передбачає використання передових технологій шифрування, багаторівневих систем автентифікації та постійного моніторингу загроз [2].

В умовах сучасних конфліктів інформація стала потужною зброєю. Маніпуляція даними, фейки, пропаганда можуть впливати на громадську думку, створювати соціальну нестабільність та підірвати довіру до державних інституцій. Тому інформаційна безпека є важливою складовою національної стратегії.

В епоху цифровізації зростає ризик витоку та несанкціонованого використання персональних даних громадян. Законодавчі ініціативи спрямовані на захист конфіденційної інформації та підвищення відповідальності компаній за її обробку.

Проте розвиток цифрових технологій створює не лише нові можливості, а й нові

виклики для національної безпеки. Захист державних інформаційних ресурсів, боротьба з кібератаками та інформаційними загрозами – це критично важливі завдання, які стоять перед будь-якою країною.

Серед основних викликів, які постають перед державами у сфері інформаційних технологій, можна виокремити:

– кіберзлочинність;

– інформаційна безпека та гібридні загрози;

– державне шпигунство;

– технологічна залежність тощо.

Один із важливих аспектів використання інформаційних технологій у сфері національної безпеки – це кібербезпека. Вразливість цифрових систем робить державні органи, підприємства та громадян мішенню для хакерських атак. Злам державних баз даних, розповсюдження шкідливого програмного забезпечення та втручання в критичну інфраструктуру можуть мати катастрофічні наслідки. Саме тому уряди розробляють стратегії кіберзахисту, впроваджують новітні системи шифрування та використовують штучний інтелект для виявлення загроз. Кіберзлочинність у державах – це зростаюча активність хакерських угруповань, які можуть атакувати державні установи, банківську систему та підприємства.

Інформаційна війна стала одним із головних викликів сучасності. Пропаганда, дезінформація та кібератаки використовуються для дестабілізації країн, маніпулювання суспільною свідомістю та підриву довіри до державних інституцій. У цьому контексті інформаційні технології відіграють як позитивну, так і негативну роль.

З одного боку, цифрові платформи можуть використовуватися для поширення правдивої інформації, оперативного реагування на загрози та боротьби з фейками. З іншого боку, соціальні мережі, месенджери та новинні сайти стають інструментами інформаційної війни. Саме тому важливо розвивати навички медіаграмотності серед громадян і впроваджувати механізми протидії дезінформації.

Державне шпигунство для сьогодення – це використання технологій для збору розвідувальної інформації іншими державами.

Технологічна залежність – критична залежність від імпортного програмного забезпечення та обладнання, що може створювати вразливості у національній системі безпеки.

Перспективи розвитку інформаційних технологій у сфері безпеки – є одним із актуальних напрямів сьогодення.

Майбутнє національної безпеки нерозривно пов’язане з розвитком інформаційних технологій. Використання штучного інтелекту, блокчейн-технологій, квантових комп’ютерів і біометричних систем значно посилить захист державних ресурсів та особистих даних громадян. Також важливим є міжнародне співробітництво у сфері кібербезпеки, обмін досвідом та створення єдиних стандартів безпеки.

Інформаційні технології є не лише джерелом загроз, а й потужним засобом їхнього запобігання. Від рівня їхньої розробки та впровадження залежить здатність держави захищати свої національні інтереси, протидіяти кіберзлочинності та інформаційним атакам. Тому розвиток цифрової грамотності, впровадження нових технологій та посилення кібербезпеки є ключовими завданнями для будь-якої країни в сучасному світі.

Щоб ефективно захищати національну безпеку в інформаційному просторі, країни повинні застосовувати комплексні заходи, а саме:

– розвиток власних технологій;

– підвищення рівня цифрової грамотності населення;

– співпраця з міжнародними партнерами;

– створення державних кіберпідрозділів.

Розвиток власних технологій базується на створенні національного програмного забезпечення та апаратних рішень.

Підвищення рівня цифрової грамотності населення забезпечується навчанням основам кібербезпеки для запобігання фішинговим атакам та іншим видам кіберзагроз.

Співпраця з міжнародними партнерами – це обмін досвідом та інформацією про сучасні загрози між державами.

Створення державних кіберпідрозділів виокремлюється формуванням спеціалізованих структур для моніторингу та реагування на кіберзагрози.

Отже, інформаційні технології є невід’ємною частиною національної безпеки. Вони

можуть як зміцнювати державу, так і створювати потенційні загрози. У сучасних умовах важливо не лише використовувати новітні технології, а й розвивати власні рішення для захисту критично важливої інформації. Комплексний підхід, що включає законодавчі ініціативи, освітні програми та міжнародну співпрацю, дозволить створити ефективну систему інформаційної безпеки та забезпечити стабільний розвиток держави в цифрову епоху.

Інформаційні технології стали ключовим інструментом у забезпеченні національної безпеки. Вони використовуються в оборонній сфері, системах управління державою, правоохоронних органах і навіть у соціальних мережах, де формується суспільна думка. Завдяки цифровим технологіям держави можуть ефективніше захищати свої кордони, здійснювати моніторинг кіберзагроз і забезпечувати безпеку громадян.

1. Хамініч С. Ю. Імперативи економічної безпеки у сучасному світі: стратегії і загрози. *Вісник Дніпропетровського науково-дослідного інституту судових експертиз Міністерства юстиції України. Економічні науки*. 2024. №1(09). С. 46–55.

2. Мирошниченко В. В. Роль інформаційних технологій в управлінні соціально-економічними системами. *Бухгалтерський облік, контроль та аналіз в умовах інституційних змін* : зб. наукових пр. VI всеукраїнської науково-практ. конф., м. Полтава, 26 жовтня 2023 р. С. 143–145.

Олександр МОВЧАН
аспірант Класичного приватного
університету (м. Запоріжжя, Україна)

УПРАВЛІННЯ КРИЗОВИМИ СИТУАЦІЯМИ В КОНТЕКСТІ ГІБРИДНИХ ЗАГРОЗ

Сучасний світ стикається з новими формами конфліктів, де традиційні військові дії поєднуються з економічним тиском, кібератаками та інформаційною війною. Такі гібридні загрози створюють кризові ситуації, які вимагають швидкого, скоординованого та ефективного управління. У цій доповіді ми розглянемо, що таке гібридні загрози, як вони впливають на кризові ситуації, та які підходи до їх управління застосовуються сьогодні.

1. Поняття гібридних загроз та їх особливості. Гібридні загрози – це комплексний набір дій, спрямованих на дестабілізацію держави чи суспільства, який поєднує військові та невійськові методи. Їх головні ознаки:

– багатовимірність: використання армії, пропаганди, економічного тиску, кібератак одночасно;

– непередбачуваність: дії часто приховані або замасковані під «внутрішні проблеми»;

– асиметричність: слабша сторона може ефективно протистояти сильнішій за допомогою неконвенційних методів.

Прикладом є агресія росії проти України: анексія Криму супроводжувалася дезінформацією, кібератаками та економічним шантажем (обмеження газопостачання). Гібридні загрози провокують кризи, які складно ідентифікувати та нейтралізувати через їх розпорошеність.

2. Вплив гібридних загроз на кризові ситуації. Кризові ситуації в контексті гібридних загроз мають декілька особливостей:

а) швидке поширення: інформаційні атаки через соціальні мережі (фейкові новини, паніка) можуть охопити мільйони людей за години. Наприклад, під час пандемії COVID-19 дезінформація про вакцини ускладнила боротьбу з кризою;

б) складність виявлення джерела: кібератаки чи фінансування протестів часто приховані через проксі-серверів чи підставних осіб, що ускладнює реагування;

в) економічні та соціальні наслідки: блокування інфраструктури (портів, енергосистем) чи санкції призводять до економічного спаду, безробіття та протестів. В Україні блокада Азовського моря у 2018 році завдала збитків експортерам;

г) психологічний тиск : постійна загроза війни чи тероризму деморалізує населення, знижуючи довіру до влади.

Ці фактори роблять управління кризами в умовах гібридних загроз значно складнішим, ніж у традиційних конфліктах.