УДК 351.86:338.49

А. Т. Ковальчук

КОНЦЕПТУАЛЬНИЙ ПІДХІД ДО ВИЗНАЧЕННЯ НАПРЯМІВ МІНІМІЗАЦІЇ АГРЕСИВНОГО ВПЛИВУ РОСІЙСЬКОЇ ФЕДЕРАЦІЇ НА ЕНЕРГЕТИЧНІ ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Досліджено проблему, пов'язану з тим, що бракує систематизованого підходу до оцінювання загроз і наслідків атак на об'єкти критичної інфраструктури України. Запропоновано новий методологічний підхід до оцінювання агресивного впливу на об'єкти критичної інфраструктури у вигляді узагальненої вербальної моделі реакції системи об'єктів критичної інфраструктури на вплив засобів агресії (на прикладі енергетичних об'єктів). Розглянуто дві тенденції мінімізації наслідків агресивного впливу на систему об'єктів критичної інфраструктури: адаптація системи до умов агресії та активний вплив на засоби агресії (вогневе ураження). Викладено пропозиції щодо шляхів подолання енергетичної кризи та обґрунтовано необхідність комплексного підходу до забезпечення стійкості критичної інфраструктури.

Ключові слова: *об'єкти критичної інфраструктури, агресивний вплив, енергетична криза, стійкість критичної інфраструктури, мінімізація впливу.*

Постановка проблеми. Російська агресія, що супроводжується постійними ракетними і кібератаками на об'єкти критичної інфраструктури (ОКІ) України, становить серйозну загрозу для національної безпеки, економічної стабільності та життєдіяльності населення. Критична інфраструктура, зокрема енергетичні, транспортні, комунікаційні та інформаційні системи, є особливо вразливою до цілеспрямованих атак, які можуть призводити до значних втрат людських життів, економічних збитків та порушення функціонування суспільства.

На сьогодні є потреба у чіткій концепції визначення напрямів мінімізації впливу агресивних дій російської федерації (рф) на ОКІ України. Через те, що бракує систематизованого підходу до оцінювання загроз і наслідків атак на ці об'єкти, ускладнюється процес прийняття управлінських рішень щодо їхнього захисту та відновлення. Крім того, відомі методи захисту не завжди враховують новітні загрози, такі, як кібератаки та дезінформаційні кампанії, що робить систему критичної інфраструктури більш уразливою. Розв'язання цієї проблеми сприятиме підвищенню стійкості України до агресивних дій з боку рф та зміцненню національної безпеки в цілому.

Аналіз останніх досліджень і публікацій. На цей час є велика кількість наукових праць, в яких розкрито певні аспекти проблем захисту ОКІ.

Зокрема, на теоретико-методичних основах забезпечення системи захисту ОКІ зосереджено увагу у працях Д. Г. Бобро [1, 2], О. М. Суходолі [3]; вивченням державної системи захисту критичної інфраструктури в Україні займалися Я. Я. Пушак, М. І. Флейчук, В. І. Франчук [4]; аналіз закордонного досвіду наводять В. О. Євсєєв [5], О. П. Єрменчук [6, 7], С. С. Теленик [8]; організаційно-технічні засади і тактичні аспекти побудови системи інженерного захисту ОКІ розглянуто у статті М. В. Коваля, В. І. Коцюруби [9]; проблему захисту ОКІ від кібератак досліджували такі науковці, як К. О. Черевко, Д. В. Пашнєв [10].

Водночас є потреба у системному підході до визначення напрямів мінімізації агресивного впливу на ОКІ, а також удосконалення способів та методів для забезпечення їхнього стійкого функціонування в умовах перманентних загроз.

Мета статті – визначення концепції мінімізації впливу російської федерації на об'єкти критичної інфраструктури та надання пропозицій щодо її практичної реалізації.

Виклад основного матеріалу. Відповідно до п. 13 ст. 1 Закону України «Про критичну інфраструктуру» об'єкти критичної інфраструктури – це сукупність важливих для економіки, національної безпеки та оборони об'єктів інфраструктури, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам [11].

Наведеним Законом (п. 4 ст. 9) визначено життєво важливі функції та послуги, порушення яких призводить до негативних наслідків для національної безпеки України, зокрема: урядування та надання найважливіших публічних (адміністративних) послуг; енергозабезпечення (у тому числі постачання теплової енергії); водопостачання та водовідведення; продовольче забезпечення; охорона

здоров'я; інформаційні послуги; електронні комунікації; фінансові послуги; транспортне забезпечення; оборона, державна безпека; правопорядок, здійснення правосуддя, тримання під вартою; цивільний захист населення та територій, служби порятунку та ін. [11].

Серед основних ОКІ, які були уражені рф в Україні з початку повномасштабного вторгнення, можна виділити такі.

1. Об'єкти енергетичної інфраструктури. Російські окупаційні війська (РОВ) завдають регулярних ударів по електростанціях, підстанціях, теплогенеруючих об'єктах та електричних мережах, що спричиняє масові перебої у постачанні електроенергії. Це зумовило виникнення масштабної енергетичної кризи, особливо в зимовий період. Знищення або пошкодження об'єктів генерації електроенергії, таких, як теплоелектростанції (ТЕС) та гідроелектростанції (ГЕС), призводить до зниження виробничих потужностей і створює значний дефіцит енергетичних ресурсів.

2. Об'єкти транспортної інфраструктури. РОВ завдають удари по залізничних станціях, мостах, дорогах та аеропортах, що порушує логістичні ланцюги, ускладнює перевезення вантажів та військової техніки, а також перешкоджає евакуації цивільного населення з небезпечних зон. Цілеспрямовані атаки на мости мають за мету порушити мобільність Сил оборони України (СОУ) і цивільних структур та максимально ускладнити постачання товарів і військової допомоги.

3. Об'єкти комунікаційної інфраструктури. РОВ атакують об'єкти зв'язку, включно з телевежами, інтернет-хабами та мобільними мережами. Це спричиняє порушення в роботі телекомунікаційних мереж, що ускладнює координацію дій як СОУ, так і цивільних структур, насамперед підрозділів Державної служби України з надзвичайних ситуацій. Крім того, рф також здійснює масштабні кібератаки на українську критичну інфраструктуру, що спрямовані на виведення з ладу інформаційних систем, дезорганізацію комунікацій та створення хаосу.

4. Системи забезпечення водопостачання і водовідведення. Удари РОВ по водозабірних та насосних станціях призводять до перебоїв у постачанні води у населені пункти, що спричиняє гуманітарну кризу, особливо в регіонах, де доступ до води є критично важливим.

5. Об'єкти системи охорони здоров'я. РОВ атакують лікарні, поліклініки та інші медичні установи, що ускладнює надання медичної допомоги і призводить до погіршення умов для лікування поранених та хворих.

6. Об'єкти нафтової і газової промисловості. Збитки нафтогазової інфраструктури оцінюються у $3,3 млрд. РОВ знищили практично всі нафтопереробні заводи в Україні та значну частину інфраструктури для зберігання нафти і нафтопродуктів [12].

7. Об'єкти оборонно-промислового комплексу.

8. Об'єкти агропромислового комплексу.

Загалом, російські атаки на ОКІ України мають комплексний і руйнівний вплив на державу, створюючи численні виклики у різних сферах життя та підвищуючи рівень гуманітарної кризи в країні.

Вплив рф на ОКІ України можемо розглядати в контексті оцінювання його наслідків, серед яких необхідно виділити такі, як: енергетична криза, зниження економічної активності, гуманітарна криза, загроза екологічної катастрофи, зниження національної стійкості українців.

Енергетична криза в Україні, що супроводжується блекаутами і віяловими вимкненнями, є прямим наслідком атак на критичну інфраструктуру. Станом на травень 2024 р. Київська школа економіки (KSE Institute) оцінює прямі збитки і непрямі фінансові втрати українського енергетичного сектору від війни у $56,2 млрд [12].

Найбільші збитки стосуються об'єктів генерації електроенергії ($8,5 млрд), магістральних електричних мереж ($2,1 млрд). Під час повномасштабного вторгнення було захоплено понад 18 ГВт електрогенеруючих потужностей, включно з найбільшою атомною електростанцією в Європі – Запорізькою АЕС. Крім того, повністю зруйновано Каховську і Дніпровську ГЕС, а також Зміївську і Трипільську ТЕС. Приватні теплоелектростанції, такі, як Ладижинська, Бурштинська, Добротвірська, Курахівська, Криворізька та Придніпровська ТЕС, зазнали серйозних пошкоджень – понад 80 %. Близько половини високовольтних підстанцій також пошкоджено [12].

Руйнування ключових об'єктів ускладнило забезпечення стабільного енергопостачання. Система енергетичного балансування стала менш надійною, що спричинило значні труднощі в забезпеченні попиту на електроенергію, особливо під час пікових навантажень. В умовах дефіциту власних виробничих потужностей Україна була змушена збільшувати імпорт електроенергії із сусідніх країн, що підвищувало витрати та залежність від зовнішніх постачальників.

Військові дії продемонстрували, наскільки вразливими є енергетичні ОКІ перед зовнішніми загрозами. Окупація і руйнування ключових енергогенеруючих об'єктів, таких, як ТЕС і ГЕС, зруйновані нафтопереробні заводи й електричні мережі підтверджують, що рівень захищеності критичних елементів інфраструктури від фізичних атак є недостатній. Захист енергетичних об'єктів не обмежується лише їхньою фізичною безпекою. Потрібно також забезпечити стійкість до перебоїв і здатність швидко відновлювати постачання електроенергії навіть за умов руйнування окремих об'єктів. Це важливий аспект для підтримання функціонування державних, промислових та соціальних систем під час війни. Відновлення пошкоджених об'єктів за принципом «відбудувати краще, ніж було» [12] сприятиме підвищенню рівня безпеки та стійкості енергетичної інфраструктури.

Зниження економічної активності. Нестабільність енергопостачання внаслідок зруйнованої інфраструктури призвела до значного зниження економічної активності в Україні. Чимало промислових підприємств були змушені або повністю зупинити свою роботу, або працювати з обмеженнями, що негативно вплинуло на економіку країни. Це, зі свого боку, спричинило істотне зменшення валового внутрішнього продукту.

Гуманітарна криза, що виникла внаслідок руйнування інфраструктури, змусила багатьох людей залишити свої домівки, спричинивши нову хвилю внутрішньо переміщених осіб. Руйнування транспортної інфраструктури призвело до серйозних перебоїв у логістиці, що ускладнило доставку гуманітарної допомоги до постраждалих регіонів, поглиблюючи кризу і створюючи додаткові виклики для постраждалих громад. Евакуація населення стала необхідністю для тих, хто опинився у небезпечних зонах або в регіонах, де неможливо забезпечити базові умови для життя.

У Миколаєві, населення якого становило близько 494,4 тис. осіб (станом на 1 березня 2015 р.), вода зникла після того, як російські окупанти підірвали водогін на Херсонщині. У Чернігові з населенням 294,1 тис. осіб (станом на початок 2016 р.), де водопостачання забезпечується зі свердловин, пошкодження насосної станції внаслідок російських обстрілів призвело до відключення води у місті.

Відповідно до Постанови Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 (у ред. від 16 січня 2024 р. № 48) час відновлення функціонування послуги з централізованого питного водопостачання у штатному режимі для більш як 145 тис. жителів не може перевищувати 24 години, рівень негативного впливу оцінюється як такий, що має катастрофічні наслідки (4 бали) [13].

Ситуація з водопостачанням у містах, таких, як Миколаїв і Чернігів, засвідчила, наскільки вразливими є елементи критичної інфраструктури під час війни. Це змушує задаватися питанням: що саме необхідно захищати найперше – самі об'єкти чи їхні функції? Адже захист об'єктів полягає у мінімізації ризиків, зниженні рівня їхньої вразливості та зменшенні наслідків. Натомість, коли йдеться про захист функцій, основна мета полягає у забезпеченні їхньої безперервності та швидкому відновленні у випадку порушення функціонування об'єктів [2].

Це свідчить про те, що, окрім фізичного захисту об'єктів, треба також мати резервні плани для відновлення критичних функцій, як це спостерігається у випадках забезпечення водопостачанням.

Загроза екологічної катастрофи, що є серйозною проблемою, яка виникла внаслідок війни. Знищення промислових об'єктів та енергетичної інфраструктури призвело до викидів шкідливих речовин, що негативно впливає на довкілля. Ракетні обстріли й інші військові дії також завдали шкоди природним ресурсам, зокрема лісам, річкам та іншим природним об'єктам, що додатково ускладнило екологічну ситуацію. Підрив російськими окупантами Каховської ГЕС став терактом з наймасштабнішим впливом на природні екосистеми з усього, що відбувалося в Україні з 24 лютого 2022 р. [14]. Його наслідки для дикої природи, економіки, енергетики, населення та загалом для національної безпеки України катастрофічні. Один із найбільших впливів цієї катастрофи – вплив на рибні ресурси: Україна втратила величезні рибні запаси [14]. Проте не дослідженим також залишається вплив на території природно-заповідного фонду, на природоохоронні об'єкти міжнародного значення, затоплення річок, опріснення та забруднення Чорного моря та ін.

Зниження національної стійкості українців. Безпека і захист ОКІ, що охоплюють стабільне постачання продовольства, водопостачання, енергопостачання, теплопостачання; кібербезпеку; стійке функціонування транспортної системи; безпеку та безперебійне функціонування інформаційних служб та служб зв'язку; забезпечення оборони та правопорядку; здатність системи охорони здоров'я функціонувати в умовах підвищеного стресу, є одним з основних елементів системи національної стійкості України [15].

Руйнування об’єктів критичної інфраструктури має значний вплив на національну стійкість України, оскільки вони забезпечують базові життєві потреби населення, стабільність державних інституцій та економіки. Втрата доступу до енергетики, водопостачання та теплопостачання залишає мільйони людей без необхідних ресурсів для виживання, особливо у холодний період року. Це підвищує смертність, знижує моральний дух суспільства та створює серйозні соціальні виклики. Зупинення роботи підприємств через перебої у постачанні електроенергії чи інших ресурсів спричиняє економічні збитки, зростання безробіття та падіння рівня життя населення. Постійна загроза атак на інфраструктуру посилює відчуття небезпеки, страху та недовіри до здатності держави забезпечити захист і безпеку громадян.

Отже, руйнування критичної інфраструктури послаблює національну стійкість України, посилюючи її вразливість до зовнішніх і внутрішніх загроз.

Адаптація системи ОКІ до зовнішніх загроз передбачає, по-перше, оцінювання реального стану системи і наслідків агресивного впливу, по-друге, – визначення напрямів мінімізації впливу зовнішніх загроз за обмежень, які притаманні цій системі.

Оцінювання наслідків агресивного впливу рф на систему ОКІ України передбачає насамперед визначення показника ефективності цієї системи $Q(u),$ який залежить від стану u ОКІ країни.

Основною вимогою під час вибору такого показника ефективності $Q(u)$ є його відповідність меті функціонування системи, яка відображується потрібним (еталонним) результатом Y_0.

Для оцінювання відповідності реального стану системи $Y(u)$ потрібному Y_0 необхідно ввести числову функцію на множині результатів *u*, яка являє собою функцію відповідності і дорівнює:

$$\rho = \rho\left[Y(u), Y_0\right], \tag{1}$$

де $Y(u)$ – реальний стан системи, яка об’єднує параметри *u* ОКІ;

Y_0 – потрібний (еталонний) стан системи.

Вид функції відповідності (1) залежить від конкретної мети функціонування системи, що досліджується, та завдання дослідження.

У загальному випадку стан системи $Y(u)$ може бути випадковою величиною. Тому функція відповідає виразу (1), як числова функція випадкового процесу також буде випадковою. Якщо результат виражається випадковою змінною, то розподіл $\Upsilon(u)$ залежить від параметрів (стратегії) *u*.

Отже, на основі поняття функції відповідності (1) за критерій ефективності системи $Q(u)$ необхідно прийняти усереднену величину:

$$Q(u) = \mathrm{M}\left\{\rho\left[Y(u), Y_0\right]\right\}, \tag{2}$$

де $\mathrm{M}\{*\}$ – операція обчислення математичного сподівання по випадковому аргументу *u*.

Якщо $Y(u)$ і Y_0 – невипадкові змінні, то функція (2) набирає такого вигляду:

$$Q(u) = \rho\left[Y(u), Y_0\right].$$

Інфраструктура держави Y_0 являє собою багатовимірну систему, яка об’єднує кінцеву множину локальних підсистем (структур) $Y_i(u) : Y_i(u) \in \Omega_Y$,

$i \in \left[1, N\right]$; де N – загальна кількість елементів інфраструктури.

У цьому випадку для оцінювання ефективності системи подібного класу необхідно використовувати векторний показник, який об’єднує показники ефективності локальних підсистем інфраструктури:

$$Q(u) = \left[Q_1(u), Q_2(u), \ldots Q_i(u) \ldots Q_N(u)\right], \tag{3}$$

де $Q_i(u), i \in [1, N];$ – часткові характеристики результату, що визначаються відповідно до формули (2) і дорівнюють:

$$Q_i(u) = \mathrm{M}\left\{\rho\left[Y_i(u), Y_i^0\right]\right\}, i \in [1, N].$$

Перехід до векторного показника ефективності системи (3) накладає додаткові вимоги щодо адекватності моделі системи, яка досліджується, за мінімальної кількості часткових показників $Q_i(u), i \in [1, N]$.

Показник ефективності системи $Q(u)$ залежить від параметрів (стратегії розвитку) об'єктів *u*, які входять до системи критичної інфраструктури. Він визначається на множині допустимих параметрів (стратегій) $\Omega_u : u \in \Omega_u$. У загальному випадку ця залежність задається відображенням множення допустимих параметрів (стратегій розвитку) системи Ω_u і множиною значень показників її ефективності:

$$F : \Omega_u \to Q(u).$$

Фактично відображення F відповідає тим чи іншим заходам (стратегіям) розвитку критичної інфраструктури і задається у формі, що визначена певною математичною моделлю системи.

Концептуальний результат методологічного підходу до оцінювання агресивного впливу на ОКІ подано на рисунку 1 у вигляді узагальненої вербальної моделі реакції системи ОКІ на вплив засобів агресії (на прикладі енергетичних об'єктів). Відповідно до цієї моделі природними вбачаються дві тенденції мінімізації наслідків агресивного впливу на систему ОКІ, а саме:

1) адаптація системи ОКІ до умов агресії, при цьому треба виділити пріоритет комплексування методів параметричної, структурної та альтернативної адаптації системи;

2) активний вплив на зовнішні засоби агресії СОУ і насамперед – їх вогневе ураження.

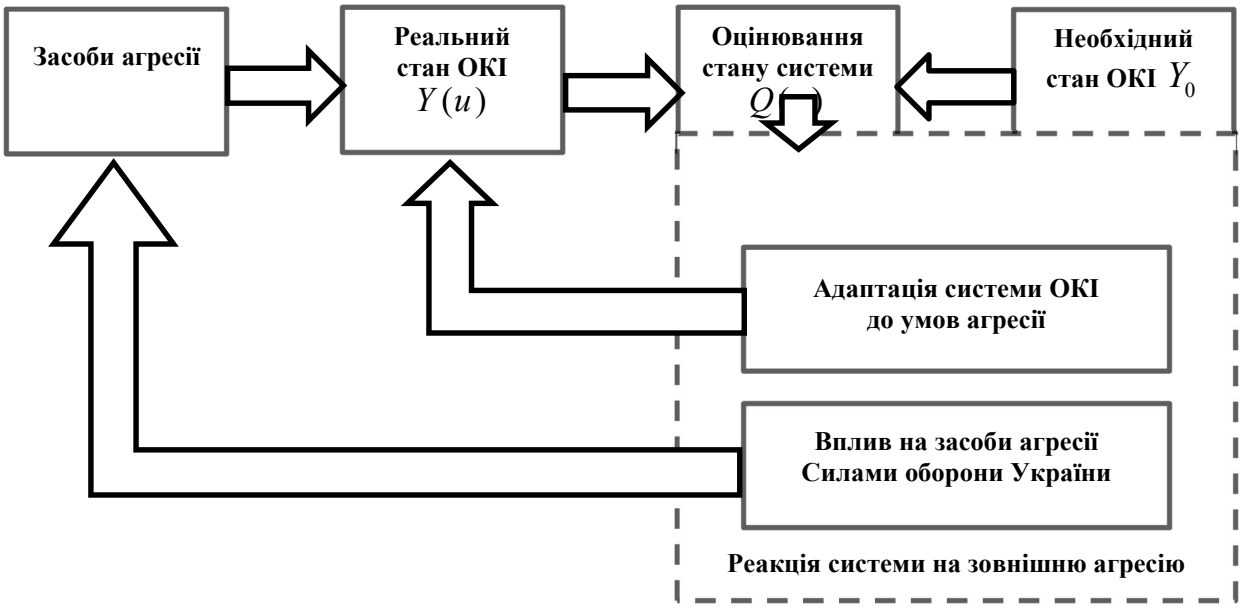

Рисунок 1 – Узагальнена вербальна модель реакції системи ОКІ на вплив засобів зовнішньої агресії (на прикладі енергетичних об'єктів)

Зображена на рисунку 1 вербальна модель певною мірою ідеалізована. Відомо, що ідеалізація притаманна будь-якій моделі, однак подана модель ураховує ключові чинники, які визначають реакцію (поведінку) системи ОКІ в умовах зовнішньої агресії, і може бути предметом подальших досліджень. Особливий інтерес становить проблема комплексування методів параметричної, структурної та альтернативної адаптації системи.

Збитки енергетичного сектору України внаслідок війни є колосальними, і тому є потреба комплексного підходу до відновлення. При цьому процес реконструкції має не лише повернути втрачене, а й підвищити стійкість до майбутніх ризиків.

З огляду на зазначені збитки й ускладнене забезпечення електроенергією населення та ОКІ виникає необхідність термінових і стратегічних дій для відновлення стабільності та забезпечення стійкості енергетичної системи.

Стійкість критичної інфраструктури – стан критичної інфраструктури, за якого забезпечується її спроможність функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після впливу загроз будь-якого виду [11]. У цьому контексті для подолання енергетичної кризи необхідно вжити таких комплексних заходів, які охоплюють як короткострокові, так і довгострокові стратегії, зокрема: невідкладне відновлення інфраструктури, оптимізація використання ресурсів, диверсифікація джерел енергії, зміцнення інфраструктури, міжнародна допомога та довгострокове планування.

Далі розглянемо практичні шляхи адаптації енергетичної системи до агресивного впливу рф на ОКІ України.

По-перше, треба вжити невідкладних заходів для забезпечення стабільності системи, а саме оперативний ремонт і відновлення пошкоджених об’єктів, таких, як електростанції та підстанції, а також мобільні генератори для підтримки критичних об’єктів. У випадку значного дефіциту електроенергії Україна може збільшити імпорт із сусідніх країн. Віялові вимкнення також можуть бути частиною стратегії для мінімізації негативного впливу на економіку та суспільство.

По-друге, важливо оптимізувати використання енергетичних ресурсів шляхом запровадження програм енергоефективності, модернізації будівель та заміни неефективних приладів. Довгострокове рішення передбачає диверсифікацію джерел енергії, розвиток відновлювальних джерел і, за можливості, розширення атомної енергетики. Це дасть змогу зменшити залежність від традиційних і вразливих до атак видів генерації.

По-третє, необхідно зміцнити енергетичну інфраструктуру, захищаючи критичні об’єкти та модернізуючи мережі. Установлення систем протиповітряної оборони, розосередження генерації і впровадження смарт-мереж для автоматичного управління потужностями можуть значно підвищити стійкість системи.

Крім того, доцільно розвивати міжнародне співробітництво в енергетичному секторі, оскільки міжнародна допомога та координація відіграють важливу роль. Залучення фінансової та технічної підтримки від міжнародних інституцій, а також обмін досвідом можуть допомогти в ефективному відновленні та захисті енергетичної інфраструктури.

Треба так само пам’ятати і про довгострокову перспективу розвитку енергетичного сектору в Україні. Для цього потрібно розробити стратегію енергетичної безпеки, інвестувати у наукові дослідження та новітні технології. Це сприятиме забезпеченню стійкості енергетичної системи України та її здатності протистояти майбутнім викликам.

Щоб подолати поточну енергетичну кризу і забезпечити стійкість енергетичної системи, Україні необхідно запровадити низку стратегічних заходів. Відновлення інфраструктури, оптимізація використання ресурсів, диверсифікація джерел енергії, зміцнення інфраструктури та міжнародна підтримка – усі ці елементи є важливими для стабілізації ситуації.

Однак для ефективного вирішення проблеми енергетичної безпеки не можна обійтися без активної участі Сил оборони України, які відіграють критичну роль у забезпеченні захисту енергетичної інфраструктури та підтримці національної безпеки в умовах проведення російською федерацією повітряних атак. Дії СОУ у сфері протиповітряної оборони, авіаційної та артилерійської підтримки, кіберзахисту, розвідки та спеціальних операцій, а також модернізації техніки є ключовими для успішного подолання енергетичної кризи та забезпечення стабільності енергетичної системи країни.

Основними шляхами, якими СОУ можуть здійснювати вплив на засоби агресії (рисунок 1) з метою подолання енергетичної кризи, є такі: 1) зміцнення протиповітряної оборони (ППО): розгортання систем ППО навколо основних енергетичних об’єктів для захисту від ракетних ударів, підвищення готовності до реагування на загрози; підвищення ефективності системи раннього виявлення і попередження про ракетні атаки, що дасть змогу своєчасно активувати ППО і зменшити наслідки; 2) авіаційна та артилерійська підтримка: виявлення і знищення ракетних пускових установок противника, а також їхніх транспортних засобів на відстані, щоб знизити частоту й ефективність ракетних атак; знищення логістичних ланцюгів ворога (складів з боєприпасами, транспортних вузлів

та інших логістичних об’єктів, що забезпечують завдання ракетних ударів по Україні); 3) кіберзахист та інформаційні операції: забезпечення кіберзахисту енергетичних об’єктів, щоб запобігти можливим кібератакам, які можуть паралізувати роботу енергетичної інфраструктури або погіршити управління системою; виявлення та нейтралізація інформаційних кампаній противника, спрямованих на дестабілізацію ситуації в енергетичному секторі та створення паніки серед населення; 4) розвідка та спеціальні операції: використання всіх наявних засобів розвідки для виявлення місць розташування ракетних систем противника та планування операцій для їхнього знищення; проведення спеціальних операцій на території рф з метою знищення ракетних комплексів, що загрожують українській інфраструктурі; 5) підготовка і мобілізація резервів: проведення навчань і тренувань військовослужбовців та працівників служб порятунку для підвищення готовності до оперативного реагування на нові ракетні атаки та їхні наслідки; у разі потреби застосування резервних сил для посилення захисту ОКІ; 6) співпраця з міжнародними партнерами: отримання додаткових засобів ППО (Patriot, IRIS-T, NASAMS), ракет дальнього радіуса дії (ATACMS, Storm Shadow/SCALP або інших високоточних ракет), що дасть змогу завдавати ударів по аеродромах, місцях базування та командних пунктах, звідки запускаються ракети, та значно підвищить здатність СОУ захищати ОКІ; активна співпраця з розвідувальними службами партнерів для оперативного обміну інформацією про можливі ракетні загрози; 7) модернізація військової техніки й озброєння: розроблення і закупівля новітніх зразків озброєння та військової техніки, а також військових технологій, які можуть підвищити ефективність захисту критичної інфраструктури, включно з безпілотними літальними апаратами, системами радіоелектронної боротьби та протиракетними комплексами; забезпечення оперативного ремонту та модернізації наявної військової техніки, що бере участь у захисті енергетичних ОКІ.

Висновки

З метою мінімізації агресивного впливу російської федерації на об’єкти критичної інфраструктури України необхідно вжити низку стратегічних та оперативних заходів з урахуванням двох тенденцій: адаптації системи об’єктів критичної інфрастуктури до умов агресії та активного впливу на засоби агресії (вогневого ураження).

Важливо посилити захист критичної інфраструктури шляхом зміцнення ешелонованої системи протиповітряної оборони, проведення модернізації засобів протиповітряної оборони та передбачити ефективні заходи для їхнього відновлення. Крім цього, необхідно нарощувати спроможності для знищення ракетних носіїв і комплексів на їхніх аеродромах та місцях базування. Це дасть змогу знизити ймовірність успішних атак на ці об’єкти.

Децентралізація і резервування є ключовими для підвищення стійкості інфраструктури, насамперед енергетичної. Перехід до більш децентралізованої системи генерації електроенергії, включно з розвитком відновлювальних джерел енергії, може зменшити вразливість до атак. Резервування критичних об’єктів, таких, як джерела енергії та водопостачання, також є важливим кроком для забезпечення безперервності функціонування у разі знищення основних об’єктів.

Посилення кіберзахисту інформаційних систем, що забезпечують роботу інфраструктури, дасть змогу запобігти кібератакам, які можуть паралізувати управління цими об’єктами. Регулярні навчання і тестування систем кіберзахисту забезпечать їхню готовність до відбиття атак.

Необхідно підвищити стійкість інфраструктури шляхом інженерної модернізації, запроваджуючи сучасні рішення для зміцнення будівель та захисту важливих об’єктів критичної інфраструктури. Упровадження автономних систем управління також дасть змогу функціонувати об’єктам незалежно від основних мереж у разі їхнього пошкодження.

Доцільно нарощувати міжнародну співпрацю у межах надання сучасних технологій та обладнання для захисту об’єктів критичної інфраструктури, а також обміну розвідувальною інформацією для вчасного реагування на загрози.

Швидке відновлення і реагування на атаки енергетичної інфраструктури в умовах війни є вкрай важливим для забезпечення стабільності країни, особливо в контексті регулярних атак противника на енергетичні об’єкти критичної інфраструктури України.

Важливо забезпечити стійкість населення за допомогою розширення інформування про загрози і засоби їхньої мінімізації.

Довгострокове і короткострокове планування, а також інвестиції у модернізацію критичної інфраструктури є необхідними для підвищення її стійкості. Розроблення стратегій безпеки і підтримка проєктів модернізації дадуть змогу зменшити вразливість і забезпечити належний рівень захисту.

Отже, застосування зазначених заходів допоможе значно зменшити агресивний вплив росії на об'єкти критичної інфраструктури України, потребує комплексного підходу і залучення ресурсів на державному, приватному та міжнародному рівнях. Це сприятиме мінімізації впливу атак на життєдіяльність країни та збереженню стійкості перед перманентними загрозами.

Подальші наукові дослідження будуть спрямовані на визначення критеріїв і показників оцінювання ефективності пріоритетних заходів мінімізації агресивного впливу на об'єкти критичної інфраструктури України.

Перелік джерел посилання

1. Бобро Д. Г. Визначення критеріїв оцінки та загрози критичній інфраструктурі. *Стратегічні пріоритети*. 2015. № 4. С. 83–93.
2. Бобро Д. Г. Методологія оцінки рівня критичності об'єктів критичної інфраструктури. *Стратегічні пріоритети*. 2016. № 3. С. 77–85.
3. Державна система захисту критичної інфраструктури в системі забезпечення національної безпеки : аналіт. доп. / за ред. О. М. Суходолі. Київ : НІСД, 2020. 28 с.
4. Криштанович М. Ф., Пушак Я. Я., Флейчук М. І., Франчук В. І. Державна політика забезпечення національної безпеки України: основні напрямки та особливості здійснення : монографія. Львів : Сполом, 2020. 418 с.
5. Євсєєв В. О. Можливі шляхи удосконалення захисту критичної інфраструктури України з урахуванням світового досвіду. *Збірник наукових праць Харківського національного університету Повітряних Сил*. 2016. № 4. С. 168–172.
6. Єрменчук О. П. Нормативно-правове регулювання діяльності у сфері захисту національної критичної інфраструктури: аналіз та узагальнення нормотворчої практики США. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2017. № 3. С. 135–140.
7. Єрменчук О. П. Основні підходи до організації захисту критичної інфраструктури в країнах Європи: досвід для України : монографія. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2018. 180 с.
8. Теленик С. С. Досвід правового регулювання системи захисту критичної інфраструктури в США. *Науковий вісник Національної академії внутрішніх справ*. 2018. № 2 (107). С. 358–370.
9. Коваль М. В., Коваль В. В., Коцюруба В. І., Білик А. С. Організаційно-технічні засади побудови системи інженерного захисту об'єктів критичної інфраструктури енергетичної галузі України. *Наука і оборона*. 2022. № 3-4. С. 11–16.
10. Черевко К., Пашнєв Д. Кібератаки на об'єкти критичної інфраструктури в умовах ведення війни: ключові поняття. *Вісник Кримінологічної асоціації України*. 2024. № 31 (1). С. 209–219. DOI: https://doi.org/10.32631/vca.2024.1.15.
11. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX: станом на 21 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 10.09.2024).
12. KSE збільшила оцінку збитків та втрат енергосектору України до $56 млрд. *Українська енергетика*. URL: https://ua-energy.org/uk/posts/kse-zbilshyla-otsinku-zbytkiv-ta-vtrat-enerhosektoru-ukrainy-do-56-mlrd (дата звернення: 10.09.2024).
13. Деякі питання об'єктів критичної інфраструктури : Постанова Кабінету Міністрів України від 09.10.2020 р. № 1109 : станом на 20 січ. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1109-2020-п#Text (дата звернення: 10.09.2024).
14. Якими є наслідки російського теракту на Каховській ГЕС для дикої природи? *Українська природоохоронна група*. URL: https://uncg.org.ua/iakymy-ie-naslidky-rosijskoho-teraktu-na-kakhovskij-hes-dlia-dykoi-pryrody/ (дата звернення: 10.09.2024).
15. Koval M. (ed.) (2023). Theoretical and applied aspects of the Russian-Ukrainian war: hybrid aggression and national resilience. Kharkiv : Technology Center PC. 372 p. DOI: http://doi.org/10.15587/978-617-8360-00-9.

УДК 351.86:338.49

А. Т. Ковальчук

CONCEPTUAL APPROACH TO DEFINING DIRECTIONS FOR MINIMIZING THE AGGRESSIVE INFLUENCE OF THE RUSSIAN FEDERATION ON UKRAINE'S ENERGY CRITICAL INFRASTRUCTURE OBJECTS

The problem associated with the lack of a systematic approach to assessing the threats and consequences of attacks by the Russian Federation on critical infrastructure facilities in Ukraine is investigated. The main critical infrastructure facilities that have been affected by the Russian occupation forces in Ukraine since the beginning of the full-scale invasion are identified. The impact of Russia on critical infrastructure facilities in Ukraine is considered in the context of assessing its consequences, among which the energy crisis, a decrease in economic activity, a humanitarian crisis, the threat of an environmental disaster, and a decrease in the national resilience of Ukrainians are highlighted. A generalized verbal model of the reaction of the system of critical infrastructure facilities (using the example of energy facilities) to the impact of means of aggression is presented as a conceptual result of the methodological approach to assessing the aggressive impact on critical infrastructure facilities. A correspondence function is proposed, which allows assessing the correspondence of the real state of the system of critical infrastructure facilities to the reference one. Two trends in minimizing the consequences of aggressive influence on the system of critical infrastructure facilities are considered: this is the adaptation of the system to the conditions of aggression and the active influence of the Defense Forces of Ukraine on external means of aggression.

Proposals are made on ways to overcome the energy crisis, namely: urgent restoration of infrastructure, optimization of resource use, diversification of energy sources, strengthening of infrastructure, international assistance and long-term planning. Particular attention is paid to the importance of the Defense Forces of Ukraine in ensuring the protection of energy infrastructure and supporting national security in the conditions of air attacks by the Russian Federation. The need for a comprehensive approach to ensuring the stability of the energy system and reducing the aggressive influence on the critical infrastructure facilities of Ukraine with the concentration of efforts at the state, private and international levels is emphasized.

Keywords: *critical infrastructure facilities, aggressive influence, energy crisis, critical infrastructure stability, impact minimization.*

Ковальчук Андрій Трохимович – начальник Військової академії (м. Одеса)
https://orcid.org/0009-0000-0907-6712