ЩОДО СТВОРЕННЯ ДЕРЖАВНОЇ СИСТЕМИ ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Сучасний стан та проблеми захисту критичної інфраструктури

Стабільне і безпечне існування держави, суспільства та його членів спирається на функціонування численних інфраструктурних об'єктів, мереж і систем, а також на можливості без перешкод отримувати доступ до важливих ресурсів. Частина з перелічених систем, об'єктів і ресурсів є настільки важливими для функціонування суспільства, економіки і держави, що їх руйнування або пошкодження призводить до негативних наслідків на загальнодержавному, а іноді й глобальному рівнях. Саме ці системи, об'єкти і ресурси відносять до критичної інфраструктури, і саме їх захист має бути першочерговим завданням для сучасної ефективної держави.

Усвідомлення світової тенденції до посилення негативних процесів природного та техногенного характеру, зростання терористичних загроз, кількості та складності кібератак, пошкодження інфраструктурних об'єктів на сході та півдні Україні, зумовлені агресивними діями Російської Федерації, актуалізували для країни питання захисту систем, об'єктів та ресурсів, життєво важливих для життєдіяльності суспільства, соціально-економічного розвитку країни та забезпечення національної безпеки.

В Україні захист об'єктів, які згідно зі світовою практикою відносять до категорії «критичної інфраструктури», регламентується численними нормативно-правовими актами, що носять переважно відомчий характер. Така ситуація обумовлена тим, що відповідні органи державної влади уповноважені реагувати лише на певні види загроз по відношенню до підпорядкованих їм об'єктів і систем, маючи у своєму розпорядженні обмежений набір інструментів та ресурсів.

Загалом на сьогодні в Україні функціонує ряд окремих державних (національних) систем, які мають відношення до захисту критичної інфраструктури у сучасному розумінні цього терміну, серед яких, зокрема:

Єдина державна система цивільного захисту (положення про систему затверджене постановою Кабінету Міністрів України від 09.01.2014 р. № 11);

Єдина систему запобігання, реагування і припинення терористичних актів та мінімізації їх наслідків (положення про систему затверджене постановою від 18.02.2016 № 92);

Державна систему фізичного захисту (порядок функціонування затверджений постановою Кабінету Міністрів України від 21.12.2011 р. №1337).

Крім того, у теперішній час на виконання положень введеної у дію Указом Президента України від 16 березня 2016 року Стратегії кібербезпеки України створюється *національна система кібербезпеки*, завдання якої тісно пов'язані із захистом критичної інфраструктури.

Гострота проблеми захисту критичної інфраструктури полягає у тому, що жодна з перелічених вище систем не призначена для реагування на усі види загроз, що обумовлює відсутність системного підходу на національному рівні до захисту критичної інфраструктури, який мав би враховувати численні взаємозв'язки її елементів. При цьому жоден орган державної влади не опікується проблемами захисту критичної інфраструктури у комплексі.

Таким чином, виходячи із потреб національної безпеки і необхідності запровадження системного підходу до розв'язання проблеми на національному рівні, створення системи захисту критичної інфраструктури є одним із пріоритетів у реформуванні сектору безпеки і оборони України на сучасному етапі.

На теперішній момент основними проблемами у сфері побудови державної системи захисту критичної інфраструктури є:

- недостатність та неузгодженість нормативно-правового регулювання в Україні захисту систем і об'єктів, які відносять до критичної

інфраструктури, зокрема, відсутність у національному законодавстві профільного закону про критичну інфраструктуру та її захист;

- відсутність на національному рівні державного органу, відповідального за координацію дій у сфері захисту критичної інфраструктури існуючих державних систем захисту та кризового реагування;
- невизначеність функцій, повноважень та відповідальності центральних органів виконавчої влади та інших органів у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів об'єктів критичної інфраструктури;
- відсутність єдиної методології проведення оцінки загроз та ризиків критичній інфраструктурі, запобігання їх реалізації та реагування на них реалізовані загрози;
- відсутність єдиних критеріїв та методології віднесення об'єктів інфраструктури до критичної інфраструктури, порядку їх паспортизації та категоризації;
- нерозвиненість державно-приватного партнерства та невизначеність джерел фінансування заходів із захисту критичної інфраструктури;
- недостатній рівень міжнародного співробітництва у цій сфері.

Зволікання з розв’язанням зазначених проблем буде не тільки гальмувати створення системи захисту критичної інфраструктури, але й створювати перешкоди для реформування та подальшого розвитку суміжних безпекових напрямів забезпечення національної безпеки.

Пріоритетні завдання створення державної системи захисту критичної інфраструктури

Вирішення проблем забезпечення захисту критичної інфраструктури потребуватиме комплексного вдосконалення правової основи діяльності органів державної влади, суб’єктів господарювання, суспільства; створення організаційно-інституційної структури функціонування державної системи управління безпекою критичної інфраструктури; визначення відповідальності,

завдань та повноважень зацікавлених суб'єктів державної системи захисту критичної інфраструктури.

У свою чергу, удосконалення правової основи захисту критичної інфраструктури потребує визначення основоположних принципів її функціонування, запровадження єдиних підходів до організації управління елементами системи на державному, місцевому та корпоративному рівнях, визначення засад взаємодії залучених державних органів та приватного сектору, суспільства та громадян, а також формування єдиної методологічно-термінологічної бази усіма суб'єктами державної системи захисту критичної інфраструктури.

За результатами опрацювання проблематики захисту критичної інфраструктури, зокрема в рамках розроблення та обговорення положень «Зеленій книзі з питань захисту критичної інфраструктури»,[1] розробленої Національним інститутом стратегічних досліджень спільно з експертами країн НАТО та ЄС з використанням кращого міжнародного досвіду пропонується наступні визначення основних термінів у сфері захисту критичної інфраструктури (Додаток 1).

Вдосконалення правової основи захисту критичної інфраструктури в Україні

Державна система забезпечення захисту та стійкості критичної інфраструктури, має гарантувати забезпечення населення, суспільства, економіки й держави життєво важливими товарами і послугами на мінімально необхідному рівні упродовж встановленого часу.

Основним завданням системи державного управління та регулювання у цій сфері є формування взаємовідносин держави, суспільства та суб'єктів господарювання з метою створення умов, що забезпечать:

---

[1] Зелена книга з питань захисту критичної інфраструктури / упоряд. Бірюков Д.С., Кондратов С.І., за заг. ред. О.М.Суходолі. – К. : НІСД, 2015. – 176 с. [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/2213/

- безперебійне стале функціонування критичної інфраструктури у різних режимах;
- спроможність запобігати руйнуванню чи завданню невиправної шкоди її елементам, припиненню їх функціонування внаслідок дії будь-яких чинників;
- швидке відновлення її функціонування після переривання у роботі.

Слід зазначити, що захист критичної інфраструктури є спільним завданням для держави, власників/операторів об'єктів критичної інфраструктури усіх форм власності, а також суспільства (населення), що вимагає, зокрема:

- надійного партнерства та співробітництва між державою, бізнесом та промисловістю на усіх рівнях;
- досягнення балансу і пропорційності між вимогами до підвищення рівня захисту, а також витратами, необхідними для реалізації цих вимог.

Дане завдання потребує утвердження «культури управління ризиками», як основи функціонування державної системи захисту критичної інфраструктури, що передбачає:

- співробітництво органів державної влади, суб'єктів господарювання та населення з питань захисту і забезпечення стійкості критичної інфраструктури;
- підвищення рівня власних спроможностей громадян, суб'єктів господарювання, установ та організацій, уразливих до припинення або погіршення функціонування критичної інфраструктури;
- запровадження системи планування на випадок виникнення кризових ситуацій (на державному і місцевому рівнях, на рівні суб'єктів господарювання та окремих установ);
- обмін інформацією між усіма суб'єктами забезпечення захисту стосовно загроз та ризиків критичній інфраструктурі;

- належний рівень міжнародного співробітництва та взаємодії із зарубіжними партнерами у сфері захисту критичної інфраструктури з огляду на глобальні та регіональні безпекові процеси і тренди.

Відповідно, пріоритетними напрямами вдосконалення правової основи діяльності державної системи захисту критичної інфраструктури слід визначити:

- створення ефективної системи державного управління у сфері захисту критичної інфраструктури, що потребуватиме створення законодавчої та нормативно-правової бази, а також прийняття інституційно-організаційних рішень в частині визначення завдань, повноважень і відповідальності залучених органів державної влади, суб'єктів господарювання та населення;
- забезпечення єдності методологічних засад діяльності суб'єктів системи державного управління у сфері захисту критичної інфраструктури, що передбачає узгодження розробки нормативно-методичних і науково-технологічних інструментів усіх залучених суб'єктів;
- розбудова державно-приватного партнерства для підвищення безпеки та забезпечення стійкості національної критичної інфраструктури, що вимагає чіткого правового врегулювання сфер відповідальності та зобов'язань держави та власників / операторів критичної інфраструктури;
- налагодження системи обміну інформацією: збір, аналіз та обробка інформації щодо загроз і ризиків для критичної інфраструктури, уразливостей та характеристик систем захисту елементів критичної інфраструктури, механізмів і процедур реагування, що включає правове врегулювання даного питання з точки зору захисту інформації з обмеженим доступом (у т.ч. розвідувальної).

Інституційні засади державної системи управління безпекою критичної інфраструктури

Для забезпечення ефективного функціонування державної системи захисту критичної інфраструктури передбачається формування нормативно-правової бази та інституційно-організаційної основи з цією метою, включаючи:

1. На загальнодержавному рівні:

- визначення органу, відповідального за координацію діяльності із захисту критичної інфраструктури в мирний час та в умовах особливого періоду;
- формування засад державно-приватного партнерства на основі взаємної довіри, належного рівня обміну інформацією, створення стимулів для інвестування у безпеку критичної інфраструктури, запровадження державою збалансованого підходу щодо вимог до підвищення рівня захисту та витрат на їх реалізацію;
- визначення функцій, повноважень та відповідальності заінтересованих органів державної влади у сфері захисту критичної інфраструктури, а також прав, обов'язків та відповідальності власників і операторів критичної інфраструктури;
- організацію взаємодії суб’єктів захисту критичної інфраструктури, обміну інформацією між ними щодо загроз і ризиків стосовно критичної інфраструктури, розбудови мережі ситуаційних центрів;
- запровадження системи підготовки та перепідготовки кадрів у сфері захисту критичної інфраструктури;
- затвердження переліку секторів критичної інфраструктури та визначення відповідальних за їх захист органів державної влади;
- визначення режимів функціонування державної системи захисту критичної інфраструктури та порядку їх зміни в залежності від змін у безпековому середовищі;
- розробку і затвердження єдиної методології проведення оцінки загроз критичній інфраструктурі;

- розробку і впровадження переліку та категорій критичності інфраструктурних елементів (об’єктів);
- розробку і впровадження методології та критеріїв віднесення інфраструктурних елементів (об'єктів) до критичної інфраструктури, порядку їх паспортизації та категоризації;
- встановлення вимог до планування заходів щодо захисту критичної інфраструктури, включаючи аварійні плани, плани взаємодії, плани відновлення критичної інфраструктури, плани проведення навчань (тренувань);
- категоризацію та паспортизацію елементів (об’єктів) критичної інфраструктури;
- розробку та затвердження Національного плану захисту та забезпечення стійкості критичної інфраструктури тощо.

2. На регіональному та галузевому (відомчому) рівнях:

- підготовка пропозицій щодо включення інфраструктурних елементів (об’єктів) до критичної інфраструктури;
- збір, узагальнення та попередній аналіз даних щодо елементів (об’єктів) критичної інфраструктури та їх функціонування;
- забезпечення функціонування відповідних систем обміну інформацією, моніторингу безпекових умов на елементах (об’єктах) критичної інфраструктури;
- участь, у встановленому законодавством порядку, у реагуванні на кризові ситуації, пов’язані з безпекою, захистом та стійкістю критичної інфраструктури;
- здійснення раннього оповіщення (попередження про загрози) власників/операторів критичної інфраструктури та надання інформаційної, консультативної, експертної, технологічної допомоги власникам/операторам критичної інфраструктури, користувачам їх послуг (населенню) задля попередження, реагування, мінімізації можливого впливу загроз;

- розроблення й упровадження стандартів, норм і регламентів захисту критичної інфраструктури у відповідних секторах критичної інфраструктури;
- здійснення перевірок та оцінки захищеності елементів (об’єктів) критичної інфраструктури;
- запровадження галузевих програм з протидії загрозам внутрішніх порушників, у т.ч. завдяки заходам, спрямованим на досягнення високого рівня культури безпеки (фізичної та технічної);
- здійснення перевірок та оцінки кібер- та інформаційної безпеки на елементах (об’єктах) критичної інфраструктури;
- участь у погодженні та обліку паспортів безпеки елементів (об’єктів) критичної інфраструктури, а також карт ризику адміністративно-територіальних одиниць тощо.

3. На місцевому рівні:

- розробку місцевих програм забезпечення захисту та стійкості критичної інфраструктури;
- розробку та погодження місцевих планів взаємодії залучених суб’єктів, планів відновлення функціонування критичної інфраструктури;
- розробку та впровадження місцевих програм підвищення стійкості громад до кризових ситуацій, викликаних припиненням або погіршенням надання важливих для їх життєдіяльності послуг, або доступу до життєво важливих ресурсів тощо.

4. На об’єктовому рівні:

- розробку та запровадження заходів із попередження кризових ситуацій;
- розробку та запровадження об’єктових планів на виконання Національного плану захисту і забезпечення стійкості критичної інфраструктури;
- формування необхідних матеріальних резервів, достатніх для реалізації об’єктових планів захисту;

- розробку, виконання та коригування об’єктових програм підвищення культури безпеки, протидії загрозам внутрішнього порушника, програм забезпечення кібер- та інформаційної безпеки;
- забезпечення відповідно до встановлених законодавством вимог конфіденційності інформації під час оброблення даних про об’єкти критичної інфраструктури;
- забезпечення відновлення функціонування критичної інфраструктури в разі виникнення аварій/збоїв, вчинення протиправних дій, або впливу природних явищ.

Організаційні засади державної системи захисту критичної інфраструктури в Україні

Державна система захисту критичної інфраструктури має багаторівневу неієрархічну архітектуру, яка відображає масштаби і комплексний характер завдань, які стоять перед нею, а також численні вертикальні та горизонтальні зв’язки, які існують між окремими елементами критичної інфраструктури.

Архітектура державної системи включає такі рівні:

1. Політичний / надвідомчий (Верховна Рада, Президент, РНБО, КМУ, створені цими суб’єктами комісії або штаби), уповноважений державою орган з координації та взаємодії суб’єктів захисту критичної інфраструктури.
2. Відомчий та регіональний (органи державної виконавчої влади визначені у встановленому законодавством порядку відповідальними за забезпечення захисту відповідних секторів критичної інфраструктури).
3. Корпоративний (власники та/або оператори критичної інфраструктури, а саме суб’єкти господарювання всіх форм власності, які забезпечують функціонування критичної інфраструктури).
4. Місцевий (місцеві органи виконавчої влади).
5. Населення та громадські об’єднання.
6. ЗМІ, експертна спільнота.

Для забезпечення узгоджених дій всієї сукупності зацікавлених осіб у сфері захисту критичної інфраструктури необхідно забезпечити правову та методологічну базу взаємодії та координації дій на різних управлінських рівнях в залежності від розвитку ситуації.

Дане завдання потребує правового та організаційного врегулювання забезпечення ефективного функціонування критичної інфраструктури в наступних режимах:

- штатний режим функціонування (здійснення оцінки можливих загроз та аналіз ризиків, інформування про імовірні загрози);
- захист та реагування на випадок реалізації загрози (задіяння, у встановленому порядку, проектних ресурсів та сил операторів та держави);
- функціонування в кризовій ситуації (залучення всіх можливих додаткових сил та ресурсів з метою забезпечення стійкості функціонування критичної інфраструктури);
- відновлення штатного режиму роботи (залучення цільових ресурсів та сил) та ліквідація наслідків кризи.

Для визначення рівня вимог до забезпечення захисту критичної інфраструктури, повноважень та відповідальності суб'єктів необхідною є категоризація елементів (об'єктів) інфраструктури. Пропонується виділення наступних груп:

І група – критично-важливі об'єкти – об'єкти, які мають загальнодержавне значення, розгалужені зв'язки та значний вплив на іншу інфраструктуру. Зазначені об'єкти включаються до переліку елементів (об'єктів) критичної інфраструктури, щодо яких на державному рівні формуються вимоги щодо забезпечення їх захисту та регламентується використання державних ресурсів та сил.

ІІ група – життєво-важливі об'єкти, порушення функціонування яких призведе до кризової ситуації регіонального значення. Зазначені об'єкти включаються до переліку елементів (об'єктів) критичної інфраструктури, щодо

яких формуються вимоги розмежування завдань й повноважень органів державної влади та власників/операторів критичної інфраструктури за забезпечення їх захисту та відновлення їх функціонування.

III група – важливі об'єкти. Пріоритетом захисту такої інфраструктури є забезпечення швидкого відновлення функцій за рахунок диверсифікації та резервів. Відповідальність за стійкість функціонування об'єктів несуть власники/оператори при встановлених законодавством вимогах щодо взаємодії із органами державної влади.

IV група – необхідні об'єкти. Об'єкти інфраструктури, яка не відноситься до критичної, безпосередній захист яких є відповідальністю оператора (власника), який має мати план реагування на кризову ситуацію.

Необхідне також детальне визначення відповідальності, завдань та повноважень суб'єктів державної системи захисту критичної інфраструктури. За результатами досліджень та вивчення кращого міжнародного досвіду пропонуються наступне розмежування завдань основних суб'єктів державної системи захисту критичної інфраструктури, зокрема:

Урядовий центр захисту критичної інфраструктури - державний орган виконавчої влади, який забезпечує функціонування державної системи захисту критичної інфраструктури: координацію взаємодії відповідних державних систем з питань забезпечення захисту критичної інфраструктури; розроблення єдиної методологічної основи функціонування державної системи; обміну інформацією між суб'єктами системи захисту критичної інфраструктури; забезпечення нагляду за дотриманням вимог законодавства з питань забезпечення захисту критичної інфраструктури.

Відомства, визначені відповідальними за сектори критичної інфраструктури, забезпечують необхідне нормативно-правове регулювання функціонування державної системи захисту у визначених секторах критичної інфраструктури, в рамках повноважень, встановлених законодавством.

Установи та відомства сектору безпеки і оборони, забезпечують охоронні та розвідувальні заходи, контррозвідувальний, контртерористичний,

кіберзахист критичної інфраструктури, обмін інформацією з питань оцінки загроз, та у взаємодії із іншими суб'єктами державної системи захисту критичної інфраструктури забезпечують реагування на загрози, кризові ситуації та ліквідацію їх наслідків.

Оператор/власник критичної інфраструктури визначається відповідальним за безпеку, захист та стійкість об'єкта критичної інфраструктури та забезпечує виконання відповідних нормативно-правових актів з цих питань, бере активну участь у розбудові державно-приватного партнерства.

Власники та/або оператори об'єктів (систем) здійснюють фінансове та ресурсне забезпечення захисту критичної інфраструктури. У разі необхідності держава може надавати допомогу власникам та/або операторам критичної інфраструктури у встановленому законодавством порядку.

ВИСНОВКИ ТА РЕКОМЕНДАЦІЇ

Складне безпекове середовище України, яке характеризується, серед іншого, зростанням терористичних загроз, збільшенням кількості природних і техногенних катастроф, вимагає віднесення захисту критичної інфраструктури до пріоритетних напрямів протидії загрозам національній безпеці.

При цьому, особливу небезпеку для функціонування критичної інфраструктури можуть являти собою загрози, у ході реалізації яких кризова ситуація на одному з елементів критичної інфраструктури внаслідок різноманітних взаємозв'язків може викликати кризову ситуацію на аналогічних об'єктах або на об'єктах критичної інфраструктури іншого призначення.

Саме тому при створенні державної системи захисту, слід виходити із спроможності системи забезпечити стійкість критичної інфраструктури до загроз усіх видів, включаючи загрози природного і техногенного характеру,

загрози, спричинені протиправними діями та будь-якими комбінаціями з переліченого.

Завдання щодо створення такої системи державного управління її безпекою знайшло своє відображення у рішенні Ради національної безпеки і оборони України від 29 грудня 2016 року «Про удосконалення заходів забезпечення захисту об'єктів критичної інфраструктури», введеного в дію Указом Президента України № 8/2017 від 16 січня 2017 року.

При цьому слід звернути увагу на необхідності посилення міжнародного співробітництва у сфері захисту критичної інфраструктури, на що поряд із посиленням спроможності національних урядів забезпечувати захист критичної інфраструктури, звертає увагу резолюція Ради безпеки ООН щодо захисту критичної інфраструктури від терористичних атак від №2341 від 13 лютого 2017 року.

Виходячи із зазначеного, ***рекомендується Кабінету Міністрів України:***

якнайшвидше забезпечити розробку та прийняття Концепції створення державної системи захисту критичної інфраструктури в Україні, як основи для розроблення відповідних нормативно-правових актів і програм захисту критичної інфраструктури; забезпечення скоординованої діяльності органів державної влади, місцевого самоврядування, суб’єктів господарювання, установ та організацій, а також населення з розв'язання практичних завдань, пов’язаних із забезпеченням захисту та стійкості критичної інфраструктури;

створити робочу групу з питань розробки першочергових нормативно-правових актів щодо створення державної системи захисту критичної інфраструктури, зокрема щодо розробки та прийняття Закону України «Про критичну інфраструктуру та її захист».

Національний інститут стратегічних досліджень

Лютий 2017 р.

Додаток 1

Визначення термінів
у сфері захисту критичної інфраструктури

У цій Концепції наведені нижче терміни вживаються у такому значенні:

1) критична інфраструктура – об’єкти, системи та ресурси, фізичні чи віртуальні, що забезпечують функції та послуги, порушення яких призведе до найсерйозніших негативних наслідків для життєдіяльності населення, суспільства, соціально-економічного розвитку, обороноздатності держави та забезпечення національної безпеки;

2) елемент (об’єкт) критичної інфраструктури – об’єкт, система, ресурс інфраструктури, фізичний чи віртуальний,що є складовою критичної інфраструктури;

3) оператор критичної інфраструктури – суб’єкт господарської діяльності (юридична або фізична особа), що відповідає за поточне функціонування елемента критичної інфраструктури та який знаходиться в його власності або розпорядженні;

4) сектор критичної інфраструктури – сукупність елементів критичної інфраструктури, що мають спільну функціональну спрямованість;

5) захист критичної інфраструктури – комплекс організаційних, нормативно-правових, інженерно-технічних, наукових та інших заходів, спрямованих на забезпечення безпеки (включаючи фізичну безпеку чи захищеність) та стійкості критичної інфраструктури;

6) безпека критичної інфраструктури (англ. *safety*) – стан критичної інфраструктури, коли дія зовнішніх та внутрішніх чинників не призводить до аварій чи інших порушень її функціонування;

7) фізична безпека (захищеність) критичної інфраструктури (англ. *security*) – стан критичної інфраструктури, за якого забезпечується її спроможність протистояти загрозам, викликаних протиправними діяннями щодо критичної інфраструктури (включаючи кібератаки);

8) стійкість критичної інфраструктури (англ. *resilience*) – стан критичної інфраструктури, за якого забезпечується її спроможність надійно функціонувати у штатному режимі, адаптуватися до умов, що постійно змінюються, протистояти та швидко відновлюватися після реалізації загроз будь-якого виду;

9) державна система захисту критичної інфраструктури – сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади, органів місцевого самоврядування, операторів критичної

інфраструктури, на які покладається реалізація державної політики у сфері захисту критичної інфраструктури;

10) категорія критичності елементу інфраструктури – відносна міра важливості елемента критичної інфраструктури, класифікована в залежності від ступеня його впливу на функціонування інститутів суспільства та держави, її господарського і оборонного комплексу, життєдіяльність населення;

11) категоризація елементів інфраструктури – віднесення елементів інфраструктури до категорій критичності;

12) паспорт безпеки – документ визначеної форми, який містить структуровані дані про окремий елемент критичної інфраструктури та визначає комплекс заходів, що вживаються оператором з метою захисту цього об’єкта;

прим.: відомості, що містяться у паспорті безпеки, можуть бути віднесені до відомостей, що становлять службову інформацію, державну або комерційну таємницю;

13) кризова ситуація – ситуація, що склалася на елементі інфраструктури або у взаємопов’язаних сферах внаслідок настання події, яка призвела до порушення функціонування критичної інфраструктури, для реагування на яку та/або відновлення до штатного режиму необхідне залучення зовнішніх сил і ресурсів.