

РОЗВИТОК ЗАКОНОДАВСТВА ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕНЕРГОПОСТАЧАННЯ

Анотація

Аналітична записка розглядає проблематику нормативного врегулювання дій учасників системи енергозабезпечення на випадок кризових ситуацій. На основі аналізу законодавства ЄС пропонуються формалізовані інструменти регламентації. Окремі запропоновані інструменти деталізуються в частині вимог до документів нормативного характеру, а також їх структури та змісту. Пропонуються першочергові кроки щодо подальшого законодавчого врегулювання питань безпеки функціонування критичної енергетичної інфраструктури.

РОЗВИТОК ЗАКОНОДАВСТВА ЄВРОПЕЙСЬКОГО СОЮЗУ У СФЕРІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ЕНЕРГОПОСТАЧАННЯ

Питання пошуку шляхів формалізації вимог до учасників системи, що забезпечує функціонування критичної інфраструктури стало особливо актуальним в останні роки. Дане завдання постало через суттєве ускладнення балансування різносторонніх інтересів учасників таких систем та державами внаслідок розширення кола учасників, подальшої лібералізації ринків, їх взаємозв'язаності та зростанням рівня глобалізації.

Додаткового поштовху до пошуку шляхів унормування підходів до забезпечення стійкості функціонування енергетики надали загрози, породжені гібридними методами ведення війн нового покоління, і зокрема використання енергетики (енергопостачання), як інструменту досягнення політичних цілей окремими країнами.¹

¹ О.Суходоля, 2017. «Енергетична зброя» в умовах гібридної війни». В книзі «Світова гібридна війна: український фронт»/ за ред. Горбуліна В.П. – К: НІСД – 496 с. - С.291-300

У відповідь, передові країни світу розпочали активне формування вимог щодо забезпечення захисту та стійкості функціонування критичної інфраструктури. Завданням даної аналітичної записки є огляд розвитку законодавства ЄС в частині формування законодавчої бази та інструментів забезпечення захисту критичної енергетичної інфраструктури.

Враховуючи євроінтеграційні прагнення України та підписання Угоди про асоціацію, даний аналіз дозволить сформулювати пропозиції щодо подальшої адаптації законодавства України до вимог законодавства ЄС в частині захисту критичної інфраструктури, зокрема захисту та забезпечення стійкості критичної енергетичної інфраструктури, безпеки енергопостачання споживачів.

Розвиток законодавства ЄС з питань безпеки критичної енергетичної інфраструктури

Зокрема, в ЄС були прийняті ряд Директив та Регламентів, які передбачали розроблення ряду механізмів запобігання виникнення кризових ситуацій, які передбачали застосування інструментарію, що виходить далеко за межі чисто технічних заходів системного оператора.

Зокрема в 2004 році в частині газопостачання була прийнята Директива Ради ЄС щодо заходів забезпечення безпеки постачання природного газу.² Яка потім деталізувалась та посилювалась через регламенти ЄС, зокрема у 2010 році³ та 2017 року.⁴ В частині електропостачання у 2006 році було прийнято Директиву Парламенту та Ради ЄС щодо заходів забезпечення безпеки електропостачання та інвестицій в інфраструктуру⁵ яка у 2018 році,

² Council Directive 2004/67/EC of 26 April 2004 concerning measures to safeguard security of natural gas supply. Режим доступу: <http://eur-lex.europa.eu/eli/dir/2004/67/oj>

³ REGULATION (EU) 994/2010 of the European Parliament and of the Council of 20 October 2010 concerning measures to safeguard security of gas supply and repealing Council Directive 2004/67/EC. Режим доступу: <http://eur-lex.europa.eu/eli/reg/2010/994/oj>

⁴ REGULATION (EU) 1938/2017 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) 994/2010. Режим доступу: <http://eur-lex.europa.eu/eli/reg/2017/1938/oj>

⁵ DIRECTIVE 89/2005/EC of the European Parliament and of the Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investment. Режим доступу: <http://eur-lex.europa.eu/eli/dir/2005/89/oj>

як очікується, буде уточнена шляхом прийняття Регламенту ЄС щодо підготовки електроенергетичного сектору до ризиків реалізації різних загроз.⁶

Загалом слід відзначити позитивний вплив України (*авт. – нажаль негативного досвіду для України*), на розвиток концептуальних засад та механізмів забезпечення стійкості енергетичних систем ЄС. Перші Директиви ЄС із цього питання були прийняті внаслідок загроз та проблем ЄС, породжених станом ринкового регулювання в Україні та кризою відносин між Україною та Росією у 2004-2005 роках. Наступне удосконалення законодавства та механізмів реагування ЄС на кризові ситуації відбувалося за результатами вивчення уроків наступних криз зумовлених використанням «енергетичної зброї» Росією проти України (другої газової війни 2009 року та гібридної війни, активна фаза якої розпочалася 2013-2014 роках).

Усвідомивши загрози стійкості функціонування енергетичних систем «не технічного» плану ЄС запровадив ряд механізмів «раннього попередження», «координації та обміну інформацією», «планування запобігання, реагування та функціонування у кризових ситуаціях» тощо.

Так, Директива №67/2004, з метою координації зусиль Співтовариства для забезпечення безпеки постачання газу на випадок значного переривання поставок створювалась Газова Координаційна Група (the Gas Coordination Group). Група також ставала механізмом регулярного аналізу постачання та обміну інформацією щодо загроз постачанню газу. Також передбачалось створення трьох-етапного механізму попередження криз: заходи застосовані підприємствами газопостачання; заходи національного рівня та на рівні Співтовариства, якщо попередні заходи не могли виправити ситуацію.

Однак Директива потребувала прийняття національного законодавства країнами-членами ЄС, що не завжди виконувалось. Дану проблему було

⁶ Proposal for a REGULATION of the European Parliament and of the Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC. Brussels, 30.11.2016. COM(2016) 862 final. Режим доступу: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0862>

висвітлено «другою газовою війною» у 2009 році, що призвело до прийняття посилення законодавчого регулювання цієї сфери, шляхом прийняття Регламентів ЄС, які мають пряму дію для всіх країн, якими було запропоновано нові механізми забезпечення «безпеки постачання».

Регламент № 994/2010 вимагав ще й призначення відповідальних, за реалізацію заходів, компетентних органів. Передбачалось також розроблення, на основі ризик-аналізу, Плану попередження криз та Плану дій на випадок криз у якому визначались дії всіх залучених осіб, а також регулярний моніторинг безпеки постачання на національному рівні. Також передбачалось затвердження інфраструктурних стандартів та стандартів безпеки постачання, які серед іншого включали заходи щодо формування додаткових потужностей та об'ємів (запасів) чи напрямів транспортування, додаткових контрактів на постачання (чи продаж із сховищ додаткових об'ємів), контракти із споживачами що дозволяли переривання постачання, а також різні технічні та організаційні рішення. Встановлювались вимоги щодо ризик-аналізу, критерії безпеки постачання та рівні та механізми кризового реагування.

Регламент прийнятий наприкінці 2017 року (№ 1938/2017) уже передбачав детальну регламентацію змісту «Плану попередження криз» та «Плану дій на випадок криз», процедур залучення приватного сектору до реагування на випадок криз; визначення критеріїв рівнів кризової ситуації та встановлення вимог щодо застосування різних механізмів реагування в залежності від рівня кризи; процедури взаємодопомоги різних учасників (країн, підприємств галузі, споживачів) на рівні регіонів та Співтовариства.

В частині електроенергетики, відбувались аналогічні процеси. Прийнята Директива № 89/2005 визначала межі забезпечення безпеки електропостачання та інвестування в електроенергетичну інфраструктуру. Ця Директива стосувалась переважно технічних аспектів забезпечення стійкості функціонування енергосистем країн-членів та розширення зв'язків між системами з метою зняття обмежень національних кордонів для розвитку

спільного ринку електроенергії Співтовариства та підвищення рівня безпеки електропостачання у випадку кризових ситуацій. У 2012 році у ЄС була створена також експертна Електроенергетична Координаційна Група (the Electricity Coordination Group), яка стала форумом обміну інформацією та координації зусиль щодо забезпечення безпеки електропостачання.

Зазначена Директива до 2014 року була переважно виконана країнами-членами, шляхом врегулювання окремих завдань в рамках інших директив щодо організації ринку електроенергії та функціонування системного оператора. Враховуючи досвід розвитку законодавства у газовій сфері і уроки гібридної війни Росії проти України та ЄС, у 2016 році на заміну Директиві № 89/2005 було підготовлено проект Регламенту з фокусом на специфічних безпекових завданнях, а саме запобігання виникненню та управлінням сектором у кризових ситуаціях.

Регламент (прогнозується до прийняття у 2018 році) також суттєво посилює вимоги до суб'єктів управління на учасників ринку електроенергії щодо готовності до криз (запобігання виникнення, функціонування під час та відновлення нормального режиму після ліквідації криз), спричинених загрозами різного типу та їх комбінацій. Зокрема передбачається встановлення загальної методології визначення кризових сценаріїв, узгодження національних планів щодо готовності до ризиків, що містять національні і регіональні заходи та регіональне співробітництво. Визначаються процедури обміну інформацією та координації зусиль, правила та відповідальність за проведення ризик аналізу, а також оцінку ресурсної адекватності (достатності потужностей, гнучкості та запасів для балансування коливань виробництва/споживання електроенергії).

Загальні висновки із аналізу розвитку законодавства ЄС.

ЄС послідовно розвиває своє законодавство з питань забезпечення захисту критичної інфраструктури та безпеки цільової функції (послуги), яку ця інфраструктура забезпечує. Зокрема в частині безпеки енергопостачання спостерігається поступове посилення вимог до учасників системи

енергозабезпечення, формалізації зазначених вимог у законодавстві, а також координації зусиль різних учасників для запобігання до, реагування на та відновлення функціонування критичної інфраструктури після виникнення кризової ситуації.

Загалом можна виділити наступні механізми забезпечення стійкості функціонування енергетичних систем, які вимагаються до застосування в ЄС:

- визначення компетентного органу з питань безпеки постачання, його завдань та повноважень – тобто ідентифікація відповідального за загальну методологію реагування та контактної точки у процесі прийняття рішень;
- залучення широкого кола учасників та застосування механізмів взаємодопомоги – тобто визнання на політичному рівні пріоритетності енергозабезпечення споживачів та можливості використання ресурсів учасників енергетичних ринків (у тому числі суміжних) на доповнення до заходів та компетенції оператора енергосистем;
- здійснення ризик аналізу та розроблення можливих кризових сценаріїв функціонування енергосистем (вищим рівнем управління - національним компетентним органом, або спеціалізованим галузевим органом на рівні ЄС) – тобто визначення рівня загроз на які має бути розраховані заходи забезпечення безпеки енергопостачання з точки зору більшої системи;
- розроблення «Плану запобігання виникнення криз» та «Плану дій на випадок криз», з врахуванням залучення до заходів широкого кола учасників енергетичного ринку та застосування механізмів взаємодопомоги – тобто виділення етапів «проектної готовності» та «надзвичайної ситуації» відповідно до рівня криз;
- розроблення стандартів операційної безпеки системних операторів, «планів запобігання» та «планів дій на випадок» – тобто формалізація вимог до змісту діяльності учасників ринку відповідно до можливого рівня кризової ситуації (рівня та кола загроз), переліку заходів (в рамках

«проектних» механізмів регулювання ринку та «позапроектних» обмежувальних) тощо;

- визначення критеріїв оцінки рівня загроз та процедур прийняття рішень щодо застосування «проектних» та «позапроектних» механізмів реагування на виникнення кризових ситуацій – тобто порядку та процедур прийняття рішення щодо застосування заздалегідь визначених заходів реагування;
- забезпечення обміну інформацією та координації зусиль учасників ринку з питань забезпечення безпеки постачання – тобто формування контактних точок та регламентів та форм обміну інформацією та прийняття рішень у різних режимах функціонування енергосистем;
- проведення періодичних тестування готовності до криз – тобто створення механізму навчання та перевірки готовності учасників до реагування на кризові ситуації;
- транскордонне співробітництво та взаємодопомога (тісна координація країн-членів та системних операторів на регіональному рівні та рівні Співтовариства).

Проведений аналіз дозволяє стверджувати про узгодженість процесів формування законодавчої бази забезпечення стійкості функціонування енергетичних систем в ЄС та Україні. Подібні підходи до побудови в Україні адекватної сьогоденню державної системи забезпечення національної стійкості, і, зокрема, стійкості функціонування енергетичної інфраструктури пропонується Концепцією створення державної системи захисту критичної інфраструктури,⁷ яка реалізовується в Україні на основі розробок Національного інституту стратегічних досліджень.⁸

Запропонований інститутом та відображений у Концепції підхід має всі підстави стати основою запровадження системи національної стійкості,

⁷ Про схвалення Концепції створення державної системи захисту критичної інфраструктури. Розпорядження Кабінету Міністрів України від 6 грудня 2017 року №1009-р. Режим доступу: <https://www.kmu.gov.ua/ua/npas/pro-shvalennya-koncepciyi-stvorenniya-derzhavnovi-sistemi-zahistu-kritichnoyi-infrastrukturi>

⁸ Developing The Critical Infrastructure Protection System in Ukraine: monograph / [S. Kondratov, D. Bobro, V. Horbulin et al.]; general editor O. Sukhodolia. – Kyiv : NISS, 2017. – 184 p.

оскільки дозволяє методологічно поєднати зусилля різних існуючих державних систем захисту та реагування на кризові ситуації (системи цивільного захисту, фізичного захисту, кіберзахисту, контр терористична система тощо).

Пропозиції щодо законодавчого та нормативного врегулювання діяльності із «забезпечення стійкості».

Саме на основі підходів забезпечення захисту критичної інфраструктури пропонується формування єдиного методологічного підходу до формалізації вимог, процедур та організації діяльності з питань забезпечення стійкості критичної інфраструктури.

Зокрема пропонується виділити наступні інструменти регламентації діяльності учасників державної системи захисту критичної інфраструктури:

1. На рівні оператора інфраструктури, необхідно врегулювати вимоги до оператора (в межах його відповідальності) щодо забезпечення безпеки та стійкості критичної інфраструктури⁹:

- для формалізації та врегулювання аспектів функціонування системи щодо яких можлива кількісна оцінка рівня загроз (на основі фізичних та технічних характеристик або ймовірностей оцінок) – встановлення комплексу **інженерно - технічних та організаційних стандартів** для врегулювання заходів захисту та забезпечення стійкості, а саме: технічні умови; стандарти виготовлення та роботи устаткування; стандарти безпеки інфраструктури, стандарти енергопостачання,¹⁰ а також посадові інструкції,

⁹ Доцільно визначити оператора основної інфраструктури (у нашому випадку – енергосистеми України) відповідальним за забезпечення стійкості всієї інфраструктури яка забезпечує виконання цільової функції для кінцевих споживачів, а не тільки щодо якої оператор є власником/розпорядником

¹⁰ Зокрема такі стандарти передбачені новим законодавством ЄС щодо безпеки енергопостачання, зокрема Регламент №1938/2017, зокрема:

Інфраструктурні стандарти (ст.5 Регламенту) вимагаються від країн членів передбачити заходи запобігання переривання постачання при умові коли один найбільший елемент системи (джерело, маршрут постачання) припиняє свою роботу (критерій N-1, що розраховується за встановленою формулою), тобто потужності інфраструктури що залишається функціонувати мають забезпечити виконання функції (енергозабезпечення) у повному обсязі протягом дня найбільшого споживання (при статистичній вірогідності раз на 20 років).

Стандарти постачання (ст.6 Регламенту) вимагають вжити заходів щодо забезпечення постачання енергії захищеним категоріям споживачів за визначеного рівня загроз: (а) екстремальні температурні режими

інструкції щодо організації систем захисту, стандарти менеджменту, плани аварійного реагування тощо;

- для формалізації та врегулювання аспектів, які проблематично оцінити у кількісному вимірі (наприклад мети, місця, часу та способу цілеспрямованого порушення функціонування КІ (диверсія, кібератака) встановлення **проектної загрози** (об'єктової)¹¹ – для врегулювання дій учасників системи захисту та забезпечення стійкості КІ відповідно до ризик аналізу (оцінки рівня загроз) здійсненого на національному рівні відповідними складовими сектору безпеки і оборони;

- загальним інструментом формалізації дій оператора (стосовно прогнозуємих та непрогнозуємих аспектів) виступатиме **Комплексний паспорт безпеки** – який має визначити заходи забезпечення стійкості КІ на рівні оператора, зокрема заходи запобігання виникнення кризової ситуації,¹² протидії загрозам та забезпечення стійкості, відновлення проектного функціонування КІ.

2. На рівні сектору КІ/регіону необхідно врегулювати вимоги до оператора та інших учасників об'єднаних інфраструктурою, у випадках коли можливостей оператора не вистачатиме, зокрема:

- для формалізації вимог до діяльності операторів критичної інфраструктури – розроблення **Вимог** до організації захисту і забезпечення стійкості КІ¹³ відповідно до рівня загроз та режиму функціонування

протягом 7 днів споживання (при статистичній вірогідності раз на 20 років); період у 30 днів екстремально високого споживання (при статистичній вірогідності раз на 20 років); період у 30 днів споживання при порушенні функціонування одного найбільший елемента системи (джерело, маршрут постачання) при середніх умовах зимового періоду.

¹¹ Даний інструмент розвинений та широко застосовується у державній системі фізичного захисту ядерних установок в Україні.

¹² Стаття 19 Закону України «Про ринок електричної енергії» вимагає від системного оператора готувати Звіт у якому серед іншого проводити оцінку ризиків ОЕС України у разі настання критичних умов з використанням відповідних критеріїв оцінки, а за результатами розрахунків режимів роботи ОЕС України за найгіршими сценаріями готувати заходи із запобігання дефіциту генеруючої та передавальної потужності.

¹³ Дані «**Вимоги**» можуть бути формалізовані у вигляді Програм, Правил або Планів. Так статтею 16 Закону України «Про ринок електричної енергії» вимагається розроблення «**Правил про безпеку постачання електричної енергії**», які повинні визначати: 1) критерії/види порушень безпеки постачання електричної енергії; 2) заходи із забезпечення безпеки постачання електричної енергії; 3) заходи, що вживатимуться у випадках ризику порушення безпеки постачання електричної енергії; 4) заходи, що вживатимуться у разі порушення безпеки постачання електричної енергії; 5) заходи, обов'язкові до вжиття учасниками ринку (крім споживачів) для забезпечення безпеки постачання електричної енергії захищеним споживачам; 6) процедуру ініціювання вжиття необхідних заходів; 7) порядок застосування необхідних заходів і строк їх дії;

інфраструктури (штатний режим функціонування; режим реагування на випадок реалізації загрози; режим функціонування в кризовій ситуації; режим відновлення);

- для оцінки рівня загроз КІ – розроблення **Проектної загрози** (секторальної);

- для оцінки готовності операторів до реагування на кризові ситуації погодження **Паспорта безпеки** операторів КІ;

- для забезпечення готовності до реагування на випадок виникнення загроз порушення цільової функції розроблення **Плану захисту КІ** (*у нашому розумінні - має забезпечити заходи запобігання порушення стійкості*);¹⁴

- для забезпечення координації реагування всіх учасників на випадок кризової ситуації (оператори, учасники відповідного ринку, споживачі послуг КІ, органи влади) розробляється **План реагування** на випадок кризи;¹⁵

- для інформаційного забезпечення запобігання та реагування на загрози встановлення **Регламенту обміну інформацією**, між учасниками планів запобігання та реагування на кризові ситуації.

2. На національному рівні забезпечення КІ, необхідно врегулювати вимоги щодо довгострокового планування розвитку КІ з врахуванням прогнозу розвитку технологічних, економічних, управлінських аспектів функціонування КІ та безпекового середовища на національному та глобальному рівні,¹⁶ а можливими інструментами можуть бути зокрема:

- для оцінки рівня загроз стійкості КІ, забезпечується проведення **Ризик-аналізу**¹⁷ загроз на національному рівні та затвердження

8) порядок інформування про вжиття необхідних заходів; 9) обов'язки та відповідальність суб'єктів владних повноважень та учасників ринку щодо забезпечення безпеки постачання електричної енергії.

¹⁴ Детальніше щодо структури документу та його вимог дивись Додаток 1

¹⁵ Детальніше щодо структури документу та його вимог дивись Додаток 2

¹⁶ Доцільно визначити компетентним органом для цього комплексу питань спеціальний орган виконавчої влади (пропонується утворення Урядового центру з питань захисту та забезпечення стійкості критичної інфраструктури. Зазначений центр має забезпечувати методологічну єдність підходів щодо реагування на різні типи загроз.

¹⁷ Детальніше щодо структури документу та його вимог дивись Додаток 3.

національної Проектної загрози, на основі Сценарного планування та Розвідувальних оцінок загроз стійкості КІ;

- для встановлення вимог щодо рівня захисту КІ визначається **Перелік об'єктів КІ та Вимоги щодо забезпечення захисту та стійкості КІ;**

- для залучення ресурсів та координації зусиль на національному рівні розробляється та затверджується **Національний план захисту та забезпечення стійкості КІ, який має формалізувати заходи запобігання виникнення загроз та реагування на кризову ситуацію та відновлення стійкості функціонування КІ;**

- для методологічного забезпечення та координації діяльності учасників визначається **Національний компетентний орган у сфері забезпечення захисту та стійкості КІ.**

Рекомендації щодо першочергових кроків із законодавчого та нормативного врегулювання питання забезпечення безпеки КІ:

1. **Кабінету Міністрів України, відповідно до рішення 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, забезпечити якнайшвидшу підготовку та подання на розгляд Верховної Ради України проект Закону України “Про критичну інфраструктуру та її захист”**

2. **Міністерству економічного розвитку і торгівлі України при підготовці проекту Закону України “Про критичну інфраструктуру та її захист” врахувати пропозиції щодо запровадження вищенаведених інструментів регламентації діяльності учасників державної системи захисту критичної інфраструктури;**

3. **Міністерству енергетики та вугільної промисловості України, іншим центральним органам виконавчої влади, державним установам, відповідальним за сектори критичної інфраструктури, опрацювати питання**

щодо нормативного врегулювання діяльності із забезпечення захисту та стійкості критичної інфраструктури на секторальному (галузевому) рівні та рівні операторів/розпорядників об'єктів критичної інфраструктури.

О.М Суходоля

Відділ енергетичної та техногенної безпеки

Плану захисту критичної інфраструктури (запобігання виникнення криз)

Структура та зміст Плану¹⁸

1. Опис системи (критичної інфраструктури)

- сукупність об'єктів, мереж та ресурсів поєднаних цільовою функцією (забезпечення споживачів енергією).

2. Висновки проведеного ризик-аналізу

- оцінки ризиків критичній інфраструктурі (ризик = загроза×вразливість×наслідки) відповідно до встановленої методології. Загалом виділяються загрози: а) політичні (у тому числі війна); б) технологічні; с) комерційні (ринкові); д) соціальні; е) природні (детальніше дивись Додаток 3);
- оцінка узагальнених сценаріїв розвитку кризових ситуацій (відповідно до встановлених критеріїв).

3. Відповідність стандартам інфраструктури

- визначення критичних елементів інфраструктури, зокрема найбільшого елементу інфраструктури (критерій N-1);
- засоби, обсяги, та потужності, спроможні вчасно компенсувати втрату найбільшого елементу інфраструктури (критерій N-1) та забезпечити стандарти постачання (відповідно до встановлених вимог);
- інші запобіжні заходи, такі як підвищення взаємопов'язаності інфраструктури та можливості забезпечити диверсифікації постачання (джерел та маршрутів).

4. Відповідність стандартам безпеки постачання

- визначення заходів запобігання та реагування на кризу, що можуть бути реалізовані на ринковими механізмами (не порушуючи нормальний режим функціонування інфраструктури);
- визначення заходів запобігання та реагування на кризу, що потребують застосування неринкових заходів (запровадження обмежень на діяльність учасників), з врахуванням чіткого визначення критеріїв та процедур їх запровадження та відміни;
- визначення заходів щодо безпеки постачання захищених категорій споживачів.

5. Заходи запобігання виникнення кризи

- заходи передбачені на запобігання ризиків відповідно до ризик-аналізу (включаючи їх територіальний вимір, очікувану ефективність та результативність, економічні наслідки для споживачів);
- склад та структура інфраструктури та заходи забезпечення відповідності вимогам стандартів безпеки постачання ат інфраструктурним стандартам;
- встановлення вимог до операторів інфраструктури в частині забезпечення захисту та надійності;
- встановлення вимог проведення тренувань на випадок кризових ситуацій.

6. Подальший розвиток системи (інфраструктурні проекти)

- оцінка взаємовпливу існуючих та будівництва майбутніх об'єктів, мереж, міжсистемних зав'язків (інтерконекторів) на безпеку постачання на випадок виникнення кризових ситуацій.

7. Зобов'язання в частині безпеки постачання (у тому числі безпека постачання захищених категорій споживачів)

- визначення захищених категорій споживачів та вимог щодо їх енергозабезпечення;

¹⁸ На основі узагальнення вимог Регламенту №1983/2017, проекту Регламенту щодо готовності електроенергетичної інфраструктури та положень Концепції створення державної системи захисту критичної інфраструктури в Україні

- зобов'язання що накладаються на операторів інфраструктури або відповідних служб щодо постачання споживачів, включаючи вимоги щодо безпеки функціонування інфраструктури.

8. Узгодженість дій учасників

- визначення ролі та повноважень компетентного органу відповідального за координацію учасників системи;
- визначення кризового менеджера, його завдань та повноважень у кризовому реагуванні;
- встановлення процедур реагування учасників на випадок криз, включаючи регламент обміну інформацією, забезпечення захисту чутливої інформації;
- встановлення процедур інформування споживачів.

10. Регіональні аспекти безпеки постачання

- розроблення механізмів співпраці із іншими постачальниками (послуг на рівні, операторів інфраструктури, регіонів (країн));
- встановлення процедури звернення за допомогою до інших країн;
- встановлення процедур обміну інформацією щодо запобігання та подолання криз на регіональному та міждержавному рівні.

План реагування на випадок кризової ситуації

Структура та зміст Плану¹⁹

1. Рівні кризової ситуації

- опис етапів та вимог до функціонування інфраструктури відповідно до рівня кризи:²⁰ (Нормальне функціонування; Підвищена увага; Кризова ситуація; Посткризове відновлення²¹);
- опис ролі та відповідальності учасників реагування відповідно рівня кризи.

2. Визначення заходів відповідно рівня кризи

2.1. Нормальне функціонування (аналіз ризиків, оцінка імовірності реалізації загрози):

- опис заходів, що готуються основними учасниками залученими до функціонування інфраструктури;
- опис процедур, які застосовуються;
- опис результатів, очікуваних від застосування заходів та процедур для запобігання або підготовки до кризи;
- опис процедур обміну інформацією залучених учасників.

2.2. Підвищена увага (попередження, запобігання)

- (a) заходи реагування, які мають бути застосовані на даному етапі (*авт. – аналогічно підпунктам попереднього етапу*);
- (b) опис вимог до звітності (інформування) учасників щодо реагування на даний рівень кризи.

2.3. Кризова ситуація

- (a) встановлення переліку наперед визначених заходів як зі сторони постачальників, так і на стороні споживачів щодо забезпечення енергією споживачів у кризовій ситуації, включаючи комерційні угоди щодо компенсаційних механізмів на припинення постачання;
- (b) деталізація застосування заходів реагування на кризу, що можуть бути реалізовані на ринковими механізмами (не порушуючи нормальний режим функціонування інфраструктури);
 - короткий опис заходів та залучених учасників реагування;
 - опис процедур, що застосовуються;
 - опис результатів, очікуваних від застосування заходів та процедур для пом'якшення кризи;

¹⁹ На основі узагальнення вимог Регламенту № 1983/2017, проекту Регламенту щодо готовності електроенергетичної інфраструктури та положень Концепції створення державної системи захисту критичної інфраструктури в Україні

²⁰ **Рівень раннього попередження (попередження):** коли є конкретна, серйозна і надійна інформація, що подія може статись і ймовірно призведе до значного погіршення ситуації з поставками і, швидше за все призведе до виникнення ситуації високого ризику чи кризової (аварійної) ситуації; Рівень раннього попередження може бути активований в механізм раннього попередження.

Рівень оповіщення ризику (оповіщення): коли трапляється порушення поставок або надзвичайно високий попит газу, що має наслідком значне погіршення ситуації з постачанням, але ринок ще може регулювати порушення чи недостатність постачання переривання поставок без необхідності вдаватися до неринкових заходів.

Аварійний рівень (аварійний): у разі виключно високою попиту на газ, значного порушення поставок чи іншого значного погіршення ситуації з поставками і у випадку навіть всі відповідні ринкові механізми запроваджено, але постачання газу є недостатнім для задоволення попиту, то для забезпечення постачання газу (відповідно до встановлених вимог) додатково повинні бути застосовані не ринкові механізми.

²¹ Відповідно до Концепції створення державної системи захисту критичної інфраструктури. Розпорядження Кабінету Міністрів України від 6 грудня 2017 року № 1009-р.

- опис процедур обміну інформацією залучених учасників;
 - заходи забезпечення нерозголошення отриманої комерційної інформації, захисту чутливої інформації;
- (с) деталізація заходів реагування на кризу, що потребують застосування неринкових заходів²²:
- короткий опис заходів та залучених учасників реагування;
 - оцінка необхідності застосування заходів обмеження ринкових механізмів для подолання кризи та рівень (обсяг) їх застосування;
 - детальний опис процедур імplementації заходів цього рівня (хто і які заходи будуть застосовуватись, і хто має приймати рішення щодо запуску та відміни);
 - визначення внеску неринкових заходів, які мають застосовуватись на етапі кризової ситуації, на доповнення до заходів ринкового регулювання (включаючи компенсаційні механізми на випадок припинення постачання);
 - оцінка результативності застосування не ринкових заходів;
 - обґрунтування відповідності заходів із положеннями щодо обмеження негативного впливу прийнятих заходів: на енергопостачання (поток) на енергетичному; на ситуацію в інших країнах ЄС; на доступ до транскордонної інфраструктури (відповідно до планів реагування на кризу);
 - опис процедур обміну інформацією залучених учасників на цьому етапі;
 - заходи забезпечення нерозголошення отриманої комерційної інформації, захисту чутливої інформації.
- (d) вимоги щодо звітності учасників щодо вжитих заходів.

2.4. Посткризове відновлення (відновлення та адаптація інфраструктури до нових умов)

- (a) встановлення переліку заходів як зі сторони постачальників, так і на стороні споживачів щодо відновлення нормального режиму функціонування інфраструктури;
 - (b) визначення заходів щодо адаптації інфраструктури до нових умов функціонування, з врахуванням отриманих уроків;
 - (с) вимоги щодо звітності учасників щодо вжитих заходів.
3. **Спеціальні заходи спрямовані на безпеку систем життєдіяльності населення (в регламенті - сфера тепlopостачання)**
- визначення заходів та дій необхідних для пом'якшення негативного впливу припинення газопостачання на інші системи життєзабезпечення;
 - деталізація обсягів енергопостачання, що мають бути поставлені захищеним категоріям споживачів та заходів забезпечення таких поставок.
4. **Кризовий менеджер або кризова команда**
- Визначення ролі та встановлення детальної процедури діяльності «кризового менеджера» відповідно рівня кризової ситуації;
 - встановлення детальної процедури та заходів, які необхідно задіяти за різними рівнями кризових ситуацій, включаючи схему взаємодії та обміну інформацією;
5. **Ролі та відповідальність учасників плану реагування**
- визначення ролі та відповідальності операторів інфраструктури та споживачів та їх взаємодію із відповідними органами влади у випадку виникнення кризових ситуацій у відповідності до встановлених рівнів;

²² Орієнтовний перелік неринкових заходів (наводиться у Регламенті), для застосування у кризовій ситуації:
 (a) на стороні постачання: використання стратегічних запасів; використання альтернативних джерел енергії; генерування електроенергії на інших технологіях (видах первинного палива); термінове збільшення виробництва тощо;
 (b) на стороні споживання: оперативні заходи зниження енергоспоживання; переведення на резервні види/джерела енергозабезпечення; застосування переривних контрактів; графіки відключення тощо.

- визначення ролі та відповідальності відповідних органів влади, інших служб відповідно до задач плану реагування на різні рівні кризової ситуації.
- 6. Заходи щодо запобігання порушення встановлених режимів постачання не захищеними категоріями споживачів**
- процедури та режими (обсяги) постачання споживачів, відповідно до рівня кризи;
 - заходи контролю за режимами споживання споживачів, відповідно до рівня кризи;
- 7. Кризове тестування**
- встановлення вимог та графіків проведення тестувань на випадок кризових ситуацій.
- 8. Регіональний вимір: заходи відповідно до типу та рівня кризової ситуації; Механізми взаємодії та взаємодопомоги; Механізми солідарності між країнами**
- формування механізму забезпечення співпраці (солідарності) між країнами за різними рівнями кризової ситуації та обміну інформацією між визначеними компетентними органами.

Ризик-аналіз з питань безпеки постачання²³

1. Опис системи

Опис сукупності мереж, об'єктів та елементів які забезпечують цілісне функціонування КІ.

2. Стандарти безпеки (інфраструктурні, операційні)

Наводяться вимоги до параметрів нормального режиму функціонування КІ.

3. Ідентифікація загроз

- (a) політичні (припинення постачання енергоресурсів з третіх країн з різних причин; політичні протести (в країнах постачальниках чи транзитних країнах); війни (в країнах постачальниках чи транзитних країнах); тероризм);
- (b) технологічні (вибухи/пожари; пожеги на обладнанні; витоки; низький рівень технічного обслуговування; збої та поломки обладнання; відсутність енергоживлення; збої с систему комп'ютерного управління технологічними процесами (програмні збої, інтернет, SCADA проблеми, тощо); кібератаки; порушення внаслідок ремонтно-будівельних робіт; тощо);
- (c) комерційні/ринкові/фінансові (контрактні зобов'язання з третіми країнами (постачальниками); комерційний спір; контроль енергетичної інфраструктури структурами третіх країн, які можуть застосувати: нехтування інвестиціями у розвиток інфраструктури; диверсифікацією; порушенням вимог законодавства ЄС; ринковим ціноутворенням; випадками різкого зростання попиту; та іншими ризиками, що призведуть до неадекватного до реальної ситуації функціонування інфраструктури);
- (d) соціальні (страйки (в різних дотичних секторах, що впливають на функціонування КІ (інші галузі енергетики, транспорт тощо), диверсії, вандалізм, крадіжки тощо);
- (e) природні (землетруси, оповзні, підтоплення, шторми, лавини, екстремальні погодні умови; пожеги (у тому ззовні поблизу об'єктів КІ) тощо).

4. Проведення ризик-аналізу

- проаналізувати ризик-фактор відповідно до специфіки та актуальності для відповідного сектору КІ (*авт²⁴.- ризик = імовірність × загроза × вразливість × наслідки*);
- опис критеріїв, які використовуватимуться для визначення чи система підпадає під ризик високого/недопустимого ризику;
- визначення набору ризик-сценаріїв у відповідності до ризик-фактору та його вірогідності та опис того як таке визначення було зроблено;
- ризик-сценарії мають бути базовані на врахуванні щонайменше наступних ризиків:
 - (a) екстремальні природні загрози (явища) та такі, що трапляються рідко;
 - (b) випадкові загрози, що виходять за межі критерію безпеки N-1;
 - (c) побічні загрози, включаючи дефіцит палива;
 - (d) зловмисні цілеспрямовані атаки.
- при проведенні ризик-аналізу необхідно щонайменше необхідно враховувати наступні елементи:
 - (a) розгляд всіх регіональних та національних обставин;
 - (b) взаємовплив та кореляція ризиків у транскордонному вимірі;
 - (c) моделювання одночасних кризових сценаріїв;

²³ На основі узагальнення вимог Регламенту №1983/2017, проекту Регламенту щодо готовності електроенергетичної інфраструктури та положень Концепції створення державної системи захисту критичної інфраструктури в Україні

²⁴ Пропонується в рамках реалізації положень Концепції створення державної системи захисту критичної інфраструктури

- (d) ранжування ризиків відповідно до їх імовірності та наслідків.
- при проведенні ризик-аналізу на найближчий період (сезонний, тижневий, денний ризик-аналіз) необхідно щонайменше необхідно враховувати наступні елементи:
 - (a) невизначеність даних для аналізу, як то імовірність пошкодження потужності передачі енергії, генеруючих потужностей, екстремальність погодних умов, не прогнозованість роботи відновлюваних джерел енергії тощо;
 - (b) імовірність настання критичних ситуацій;
 - (c) імовірність настання одночасних кризових ситуацій.

5. Висновки