НІСД НАЦІОНАЛЬНИЙ ІНСТИТУТ СТРАТЕГІЧНИХ ДОСЛІДЖЕНЬ
NATIONAL INSTITUTE FOR STRATEGIC STUDIES NISS

ЦЕНТР БЕЗПЕКОВИХ ДОСЛІДЖЕНЬ
CENTER FOR SECURITY STUDIES

СТІЙКІСТЬ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЄС: ПОСИЛЕННЯ ПОЛІТИКИ ТА КООРДИНАЦІЇ

Олександр Суходоля, *д-р наук з держ. упр., проф., відділ критичної інфраструктури, енергетичної та екологічної безпеки центру безпекових досліджень НІСД*

Проаналізовано пріоритети розвитку політики ЄС щодо забезпечення стійкості критичної інфраструктури та безперервності виконання життєво важливих функцій на рівні Євросоюзу. Наголошено на узгодженості розвитку політики захисту критичної інфраструктури із безпековою політикою ЄС і НАТО з огляду на російську агресію проти України.

Висновки та рекомендації

Європейський Союз проголосив нові пріоритети політики забезпечення стійкості функціонування критичної інфраструктури (КІ) та надання життєво важливих послуг на ринку ЄС. Нові стратегічні цілі та завдання Єврокомісії та держав-членів були визначені в Рекомендаціях Ради ЄС, спрямованих на посилення зусиль ЄС щодо підвищення стійкості КІ. Нові підходи відображають прихильність ЄС до формування механізмів забезпечення безпеки та стійкості функціонування КІ на основі ринкових механізмів і стимулювання операторів КІ до активізації їхніх зусиль щодо забезпечення захисту КІ на добровільній основі.

Для підтримки цих зусиль передбачається формування низки інструментів надання допомоги державам – членам ЄС та операторам КІ. Серед таких інструментів – надання методичної та консультативної допомоги, сприяння підвищенню кваліфікації персоналу операторів КІ та проведенню стрес-тестів, координація зусиль на рівні ЄС у випадку виникнення кризової ситуації, формування інструментів фінансової підтримки діяльності в цій сфері.

Зазначені модифікації політики ЄС є важливим орієнтиром для України. Усвідомлення особливостей нових пріоритетів політики та законодавства ЄС в цій сфері мають бути належним чином опрацьовані суб'єктами національної системи захисту КІ, а подальші кроки з її розвитку мають здійснюватися з урахуванням розвитку законодавства ЄС.

Новий етап розвитку політики ЄС щодо стійкості критичної інфраструктури

Зважаючи на ймовірність виникнення нових викликів і загроз безпеці життєдіяльності, зокрема спричинених агресією РФ проти України, Європейський Союз усвідомив необхідність узгодження дій держав-членів та національних органів влади, інституцій ЄС та операторів критичної інфраструктури задля забезпечення стійкості надання життєво важливих послуг на ринку ЄС.

У грудні 2022 р. Рада ЄС ухвалила Рекомендації зі скоординованого підходу до стійкості критичної інфраструктури. Зокрема, рекомендовано запровадити необхідні інструменти та забезпечити координацію дій на рівні ЄС з підвищення готовності та реагування на безпекові інциденти, що загрожують порушенню надання життєво важливих послуг на внутрішньому ринку Євросоюзу. Огляд запропонованих цілей, інструментів та пріоритетів політики ЄС у сфері стійкості КІ наведено в *Додатку 1*.

Тоді ж Рада ЄС прийняла нову Директиву щодо стійкості критичних об'єктів (Директива *CER*). На початку 2023 р. було оголошено про синхронізацію зусиль ЄС і НАТО щодо забезпечення стійкості критичної інфраструктури[1]. Окремі інструменти регулювання та особливості нової Директиви *CER* висвітлено в *Додатку 2*.

Прийняті рішення фактично засвідчили початок нового етапу розвитку політики ЄС щодо безпеки та стійкості КІ.

Огляд нових підходів ЄС до захисту критичної інфраструктури

Нові Рекомендації Ради ЄС мають на меті підвищити ефективність політики, прискорити прийняття та імплементацію нових вимог до захисту КІ на рівні ЄС та держав-членів, запровадити єдині методологічні підходи та посилити координацію дій усіх залучених учасників.

Рекомендації встановлюють низку цілеспрямованих системних заходів законодавчого та організаційного характеру на рівні ЄС та національному рівні задля підвищення стійкості функціонування КІ. Ці зусилля пропонується зосередити на спроможності ідентифікувати загрози й ризики щодо надання життєво важливих послуг, підвищення готовності КІ до кризових ситуацій, посилення спроможності реагувати на загрози, міжнародній співпраці у сфері захисту КІ.

Реалізація Рекомендацій спрямована на значне розширення можливостей ЄС щодо забезпечення стійкості КІ. Директива *CER* окреслює чіткі вимоги й конкретні інструменти моніторингу й регулювання діяльності у сфері захисту КІ, встановлює низку нових зобов'язань держав-членів та операторів КІ щодо забезпечення стійкості функціонування критичної інфраструктури, а також розширює перелік секторів КІ, які

[1] НАТО і ЄС домовились створити Спеціальну групу з питань стійкості і захисту критичної інфраструктури. 2023. 11 січ. URL: https://www.nato.int/cps/en/natohq/news_210611.htm?selectedLocale=uk

підлягатимуть регулюванню[2]. Крім того, оновлена Директива *NIS2* також запроваджує широке охоплення секторів КІ зобов'язаннями стосовно кібербезпеки. Нове законодавство вимагає від Єврокомісії взяти на себе провідну координаційну роль та надає їй відповідні повноваження.

Метою посилення політики ЄС щодо стійкості КІ є зміцнення спроможності держав-членів підвищувати стійкість у наданні послуг, які мають вирішальне значення для підтримання життєво важливих суспільних функцій, економічної діяльності, громадського здоров'я, безпеки та навколишнього середовища у ЄС.

Підвищення стійкості КІ визнається одним із пріоритетних напрямів безпекової політики ЄС. Наголошується, що підвищення стійкості європейської КІ до загроз, створених людиною (цілеспрямованих зловмисних дій)[3], має стати пріоритетом для ключових секторів КІ, таких як енергетика, цифрова інфраструктура, транспорт та космос. Крім того, Рекомендації наголошують на пріоритетній увазі до транскордонної інфраструктури.

Щоб оцінити ризики надання життєво важливих послуг, які зумовлені антропогенними загрозами КІ, важливо мати точну, актуальну та повну картину найважливіших ризиків, з якими стикаються оператори КІ. Рекомендується: посилити вимоги до держав-членів щодо взаємодії під час проведення аналізу подібних ризиків та загроз, розширити механізми співпраці та обміну інформацією щодо таких видів діяльності, як-от ідентифікація КІ, проведення стрес-тестів КІ[4], вивчення спільних уроків зі стрес-тестів, виявлення вразливостей КІ та можливих заходів реагування.

Хоча основну відповідальність за забезпечення безпеки КІ покладено на держави, які є членами ЄС, посилення координації на рівні Євросоюзу є доречним, особливо щодо загроз, котрі можуть вплинути на кілька держав-членів одночасно. Тому планується запровадження механізмів координації в рамках ЄС. Наголошується на докладанні на міжнародному рівні зусиль для ефективного усунення ризиків та підвищення стійкості суб'єктів, які експлуатують КІ або в Союзі, або у відповідних третіх країнах, або в міжнародних водах. Відповідно, в реалізації політики ЄС щодо підвищення стійкості КІ передбачається щільна співпраця держав – членів ЄС, Єврокомісії з Високим представником ЄС із закордонних справ та безпекової політики.

---

[2] Критичними секторами визначено: енергетику, транспорт, банки, інфраструктуру фінансових ринків, інфраструктуру охорони здоров'я, постачання питної води, водовідведення (каналізацію), цифрову інфраструктуру, державне управління, космос, виробництво продовольства.

[3] У тексті Рекомендацій акцентується увага на актах диверсій на газогонах «Північний потік – 2», загрозах підводним кабелям зв'язку, та ризиках стійкості надання життєво важливих послуг на внутрішньому ринку ЄС, спричинених війною Росії проти України.

[4] Стрес-тест має бути доповнений розробкою Плану інцидентів і криз КІ, який описує та визначає цілі та способи співпраці між державами-членами та інституціями, органами, офісами та агентствами ЄС у реагуванні на пов'язані з КІ інциденти.

Додатки

Додаток 1

ОГЛЯД РЕКОМЕНДАЦІЙ РАДИ ЄС ЩОДО ЦІЛЕЙ ТА ЗАХОДІВ РОЗВИТКУ ПОЛІТИКИ У СФЕРІ СТІЙКОСТІ КРИТИЧНОЇ ІНФРАСТРУКУТРИ

1. Підвищення готовності ЄС до кризових ситуацій

1.1. Держави – члени ЄС мають:

– застосовувати методологію оцінювання ризиків КІ на основі аналізу впливу загроз будь-яких типів (*all-hazard approach*) при подальшій адаптації національних підходів до ризик-аналізу;

– розпочати розроблення заходів щодо підвищення стійкості КІ згідно з положеннями нового законодавства в цій сфері. Особливий акцент має бути на співпраці та обміні відповідною інформацією між державами-членами та Єврокомісією, виявленні загроз КІ транскордонного характеру та посиленні підтримки операторів для забезпечення стійкості КІ;

– підтримувати проведення навчань і тренінгів з питань стійкості КІ, залучати експертів, заохочувати їх брати участь у навчальних тренінгових програмах;

– заохочувати та підтримувати операторів КІ, принаймні в енергетичному секторі, проводити стрес-тести, дотримуючись принципів, узгоджених на рівні ЄС. Стрес-тести мають оцінювати стійкість КІ до цілеспрямованих руйнівних атак. Необхідно визначити відповідну КІ для перевірки не пізніше ніж у І кварталі 2023 р.;

– виділяти достатні фінансові ресурси для зміцнення спроможності відповідних національних органів, щоб мати можливість підвищувати стійкість КІ;

– використовувати потенційні можливості фінансування на рівні ЄС та держав-членів для підвищення стійкості КІ, а також заохочувати операторів КІ використовувати такі можливості фінансування. Зокрема, наголошується на доцільності використання програм, що фінансуються Фондом внутрішньої безпеки ЄС, Європейським фондом регіонального розвитку, Механізму цивільного захисту ЄС (*UCPM*), Плану *REPowerEU*, а також використовувати результати відповідних проєктів у рамках дослідницьких програм, таких як *Horizon Europe*;

– розвивати використання можливостей програми *Copernicus*, системи *Galileo* та Європейської геостаціонарної навігаційної служби (*EGNOS*) для спостереження та обміну інформацією, а також використовувати можливості, які пропонуються на рівні ЄС, зокрема Урядовий супутниковий зв'язок (*GOVSATCOM*) космічної програми ЄС, для моніторингу КІ та підтримки прогнозування кризових ситуацій і реагування на них.

1.2. На наднаціональному рівні Єврокомісія має:

– забезпечити посилення діалогу та співпраці між Єврокомісією та делегованими державами-членами експертами для обговорення завдань забезпечення безпеки та стійкості КІ, передусім щодо:

(a) сприяння підготовці, розробленню та просуванню загальних добровільних інструментів для підтримки держав-членів у підвищенні стійкості КІ, включно з методологією та сценаріями ризиків;

(b) підтримки держав-членів у впровадженні нової законодавчої бази щодо захисту КІ;

(c) підтримки проведення стрес-тестів стійкості КІ, передусім щодо актів цілеспрямованого руйнування енергетичної КІ, а також підтримки та консультування стосовно проведення таких стрес-тестів на запит держави-члена;

(d) аналізу та обміну на добровільній основі (на захищеній платформі, створеній Єврокомісією) найкращими практиками, отриманими з національного досвіду, та іншою інформацією, пов'язаною зі стійкістю КІ;

– забезпечити підтримку держав-членів, зокрема у спосіб підготовки посібників і вказівок із захисту КІ та громадських місць від безпілотних літальних систем, інструментів для проведення оцінювання загроз та аналізування ризиків, а також проводити брифінги щодо загроз КІ з метою покращення обізнаності про ситуацію;

– активізувати роботу над перспективними діями на випередження, включно зі співпрацею з державами-членами (застосування механізму «раннього попередження», *UCPM*), плануванням на випадок надзвичайних ситуацій за підтримки Центру координації реагування на надзвичайні ситуації (*ERCC*), а також підвищувати рівень оперативної готовності та реагування на збої в роботі КІ, збільшувати інвестиції в превентивні підходи та готовність населення, розбудову потенціалу в рамках Мережі знань цивільного захисту ЄС (*Union Civil Protection Knowledge Network*);

– сприяти використанню засобів спостереження Союзу (*Copernicus, Galileo* та *EGNOS*) для підтримки моніторингу критичної інфраструктури в державах-членах, а також можливостей спостереження, передбачених у Космічній програмі ЄС;

– сприяти залученню спроможностей агенцій ЄС до заходів із забезпечення стійкості КІ, зокрема: (a) Агентства Європейського Союзу зі співробітництва правоохоронних органів (*EUROPOL*) щодо збору інформації, кримінального аналізу та підтримки розслідувань у транскордонних правоохоронних діях; (b) Європейського агентства з морської безпеки (*EMSA*) з питань, пов'язаних із безпекою морського сектору, включно з послугами морського спостереження, що стосуються питань, пов'язаних із безпекою на морі; (c) Агентства Європейського Союзу з космічної програми (*EUSPA*) і Супутникового центру ЄС (*SatCen*) щодо допомоги через операції в рамках Космічної програми; (d) Європейського центру компетенції з кібербезпеки (*ECCC*) у діяльності, що пов'язана з кібербезпекою, також у співпраці з Агентством

Європейського Союзу з кібербезпеки (*ENISA*) щодо підтримки інновацій та промислової політики в галузі кібербезпеки.

2. Підвищення спроможності реагування ЄС на загрози КІ

2.1. Держави – члени ЄС мають:

– розвивати й надалі власні механізми координації залучених акторів у процесі реагування, забезпечити підготовку оглядів міжсекторального реагування на суттєві збої в основних послугах, що надаються КІ. Започаткувати розроблення плану скоординованого реагування на збої в роботі КІ зі значним транскордонним значенням;

– збільшити обмін інформацією на оперативному рівні з *ERCC* у контексті *UCPM*, щоб покращити раннє попередження та координувати реагування на збої в роботі КІ зі значним транскордонним значенням, забезпечуючи швидшу реакцію ЄС за потреби;

– заохочувати операторів КІ та відповідні національні органи влади збільшувати свій потенціал, щоб мати можливість швидко відновити виконання життєво важливих функцій, що забезпечуються операторами КІ;

– заохочувати операторів КІ під час реконструкції своєї інфраструктури будувати її так, щоб вона була максимально стійкою до повного спектра значних ризиків, беручи до уваги пропорційність заходів стосовно оцінки ризику та витрат;

– прискорити підготовку до запровадження посилених вимог щодо кібербезпеки, маючи на меті розвиток спроможностей національних *CSIRT*, збільшення кількості секторів КІ, перегляд стратегій кібербезпеки та національних планів реагування на інциденти й кризи в кібербезпеці;

– утілювати в життя заходи, спрямовані на усвідомлення відповідними зацікавленими сторонами необхідності підвищення стійкості КІ; приділяти увагу проактивним стратегічним комунікаціям у контексті протидії гібридним загрозам і кампаніям, спрямованим на КІ.

2.2. На наднаціональному рівні Єврокомісія має:

– тісно співпрацювати з державами-членами для подальшого розвитку відповідних органів, інструментів і можливостей реагування з метою підвищення оперативної готовності до усунення безпосередніх і непрямих наслідків значних збоїв у відповідних основних послугах, що надаються КІ, зокрема експертів і ресурсів, доступних через *ECPP* і *rescEU*[5] в рамках *UCPM* або майбутніх спільних груп швидкого реагування;

– у контексті *UCPM*: постійно аналізувати й перевіряти достатність та оперативну готовність наявних можливостей реагування; регулярно відстежувати й виявляти потенційно значущі прогалини у можливостях реагування *ECPP* та *rescEU*;

[5] *RescEU* є елементом механізму цивільного захисту ЄС для посилення як захисту громадян від катастроф, так і управління ризиками (*див.:* URL: https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/resceu_en).

інтенсифікувати міжсекторальну співпрацю для забезпечення адекватного реагування та організовувати регулярні навчання з метою перевірки взаємодії з однією чи кількома державами-членами; сприяти подальшому розвиткові *ERCC* як міжгалузевого центру надзвичайних ситуацій на рівні ЄС для координації підтримки держав-членів, що постраждали;

– розробити План скоординованої реакції на збої в роботі КІ зі значним транскордонним значенням, який описує та визначає цілі та способи співпраці держав-членів та ЄС, інституцій, органів, офісів та агенцій у реагуванні на інциденти в КІ.

3. Розвиток міжнародного співробітництва

3.1. Держави – члени ЄС мають співпрацювати:

– відповідно до законодавства ЄС з конкретними третіми державами щодо стійкості КІ зі значним транскордонним значенням;

– з Єврокомісією та Високим представником ЄС для ефективного усунення ризиків КІ в міжнародних водах;

– з Єврокомісією та Високим представником ЄС стосовно прискореного розроблення й упровадження інструментарію ЄС для скоординованої відповіді на гібридні кампанії та загрози, зокрема щодо КІ.

3.2. На наднаціональному рівні Єврокомісія має:

– підтримувати разом із Високим представником ЄС у відповідних випадках та згідно з їхніми завданнями та обов'язками, визначеними законодавством Союзу, відповідні треті держави для підвищення стійкості КІ на їхній території;

– посилювати координацію з НАТО щодо стійкості КІ спільного інтересу через структурований діалог ЄС – НАТО щодо стійкості, повністю поважаючи компетенції Союзу та держав-членів згідно з договорами та ключовими принципами співпраці між ЄС і НАТО;

– розглянути участь представників відповідних третіх держав, якщо це необхідно та доречно, у рамках співпраці та обміну інформацією між державами-членами у сфері стійкості КІ, яка фізично пов'язана з територією держави-члена та третьої держави.

Додаток 2

ОСНОВНІ НОВАЦІЇ ДИРЕКТИВИ *CER* ЩОДО СТІЙКОСТІ КРИТИЧНИХ ОБ'ЄКТІВ

Директива *CER* визначає загальні засади формування політики ЄС щодо стійкості виконання життєво важливих функцій. Порівняно з попередньою Директивою 2008/114/ЕС щодо ідентифікації КІ, яка анулюється, Директива *CER* зміщує акценти з «організації захисту ідентифікованої КІ» до забезпечення стійкості виконання життєво важливих функцій суб'єктами, які експлуатують критичну інфраструктуру (далі – оператори КІ).

Директива *CER* запроваджує вимоги щодо забезпечення стійкості виконання життєво важливих функцій оператором КІ, взаємодії між операторами КІ та уповноваженими державними органами на національному рівні, визначає повноваження Єврокомісії щодо координації національних зусиль та інституцій ЄС на рівні Союзу з метою забезпечення стійкості виконання життєво важливих функцій на внутрішньому ринку ЄС.

Зокрема, Директива *CER* встановлює:

– зобов'язання держав – членів ЄС вжити специфічних заходів із забезпечення послуг, які є життєво важливими для підтримання суспільних функцій або економічної активності;

– вимоги до держав ЄС ухвалити стратегію підвищення стійкості роботи операторів КІ з надання життєво важливих послуг;

– вимоги щодо проведення ризик-аналізу стійкості надання визначених послуг на рівні ЄС, національному рівні та рівні операторів КІ за всіма визначеними Директивою секторами та підсекторами КІ;

– процедуру ідентифікації операторів КІ, які забезпечують надання послуг, передусім у частині інфраструктури загальноєвропейського значення;

– зобов'язання для операторів КІ щодо підвищення їхньої стійкості та спроможності забезпечувати надання послуг, зокрема застосування операторами КІ планів стійкості, які повинні містити технічні, безпекові та організаційні заходи відповідно до визначеного рівня загроз та їхнього впливу;

– правила моніторингу виконання оператором КІ заходів із забезпечення безпеки та стійкості КІ;

– консультативно-координаційний механізм підтримки діяльності Єврокомісії та підготовки нормативних і методичних матеріалів для держав – членів ЄС та операторів КІ, а саме створення Групи стійкості операторів КІ;

– інститут «консультативної місії» для проведення оцінювання вжитих оператором КІ обов'язкових заходів із забезпечення стійкості функціонування КІ;

– механізми сприяння співпраці між державами – членами ЄС та обміну інформацією з питань стійкості виконання життєво важливих функцій;

– вимоги щодо визначення уповноваженого органу, який виконуватиме роль «точки контакту» для взаємодії між державами – членами ЄС, Єврокомісією та іншими інституціями ЄС, операторами КІ;

– підготовку методичних та інструктивних матеріалів, підтримку в організації та проведенні колективних навчань, консультування, запровадження програм підвищення кваліфікації персоналу операторів КІ;

– інші механізми забезпечення координації дій залучених інституцій щодо реалізації положень Директиви.

Положення Директиви *CER* не стосуються органів державної влади, які здійснюють свою діяльність у сферах національної безпеки, громадської безпеки, оборони чи правоохоронної діяльності. Зобов'язання, викладені в цій Директиві, не створюють вимог щодо розкриття інформації, розголошення якої суперечило б основним інтересам національної безпеки, громадської безпеки чи оборони держав-членів.