Додаток

Огляд положень
Директиви щодо стійкості надання життєво важливих послуг / функцій операторами критичної інфраструктури (Директива CER)[1]

Директива CER окреслює загальні межі формування політики ЄС щодо стійкості надання життєво важливих послуг / функцій суб'єктами, які експлуатують КІ (далі – оператори КІ), запроваджує механізми взаємодії між операторами КІ та уповноваженими державними органами на національному рівні, визначає компетенцію Єврокомісії щодо координації національних зусиль та інституцій ЄС на рівні Союзу з метою забезпечення стійкості функціонування критичної інфраструктури, котра надає життєво важливі функції / послуги *(«vital services», «essential services»*) на внутрішньому ринку ЄС.

1. Порівняно з попередньою Директивою 2008/114/ЕС щодо ідентифікації КІ, яка анулюється, Директива CER дещо зміщує акценти з «ідентифікації КІ та встановлення вимог до її захисту» до «забезпечення стійкості[2] надання оператором КІ життєво важливих послуг».

2. Директива CER формулює зобов'язання держав – членів ЄС та визначає межі реалізації національних політик щодо забезпечення стійкості надання операторами КІ життєво важливих послуг.

Зокрема встановлюється вимога до кожної держави – члена ЄС протягом трьох років з дати офіційної публікації Директиви ухвалити ***стратегію підвищення стійкості роботи операторів КІ, які забезпечують надання життєво важливих послуг***. Документ має визначити стратегічні цілі та заходи з підвищення стійкості функціонування операторів КІ відповідно до визначеної методології ідентифікації КІ.

Кожна стратегія має містити такі складові:

- стратегічні цілі та пріоритети підвищення загальної стійкості операторів КІ з урахуванням транскордонних і міжгалузевих залежностей;
- структуру управління для досягнення стратегічних цілей і пріоритетів, включно з описом ролей і відповідальності різних органів влади, операторів КІ та інших сторін, залучених до реалізації стратегії;
- перелік заходів, необхідних для підвищення загальної стійкості операторів КІ, включно з оцінкою ризиків забезпечення надання життєво важливих функцій / послуг;
- опис процесу, за допомогою якого ідентифікуються КІ та оператори КІ;

[1] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2557

[2] «Стійкість» означає здатність оператора КІ запобігати, захищати, реагувати, протистояти, пом'якшувати, поглинати, пристосовуватись і відновлюватись після інциденту.

- характеристику процесу підтримки операторів КІ, включно із заходами зміцнення державно-приватного партнерства;
- перелік основних органів влади та зацікавлених сторін, окрім операторів КІ, залучених до реалізації стратегії;
- засади координації між уповноваженими органами держав – членів ЄС з реагування на загрози різного виду та забезпечення моніторингових завдань виконання положень Директиви;
- опис чинних заходів, спрямованих на сприяння виконанню малими та середніми підприємствами – операторами КІ зобов'язань згідно з Директивою.

Держави – члени ЄС мають інформувати Єврокомісію про результати розроблення та ухвалення стратегії протягом трьох місяців з дати її прийняття. Держави мають забезпечити перегляд стратегії щонайменше раз на чотири роки.

3. Директива CER наділяє Єврокомісію повноваженням щодо деталізації переліку життєво важливих послуг у секторах та підсекторах, визначених Додатком до Директиви.

4. Директива CER встановлює вимогу щодо ***проведення ризик-аналізу стійкості надання визначених життєво важливих послуг*** (*Member State risk assessment*[3]) відповідно до визначеного переліку та періодичність його проведення – щонайменше один раз на чотири роки.

Аналіз ризиків має враховувати загрози будь-якого типу[4]. Під час його проведення держави – члени ЄС можуть використовувати чинні положення законодавства ЄС щодо ризик-аналізу, які застосовуються в енергетичній сфері, сфері контртерористичного та цивільного захисту[5]. Аналіз ризиків має враховувати загрози міжсекторального та транскордонного характеру, зокрема загрози, сформовані у третіх країнах, та оцінювати їхній негативний вплив на життєдіяльність громадян та внутрішній ринок ЄС.

Результати проведеного аналізу ризиків мають бути доступними для використання операторами КІ, визначеними згідно з установленою процедурою. Про результати проведення ризик-аналізу потрібно інформувати Єврокомісію.

5. Директива встановлює загальну ***процедуру ідентифікації операторів КІ, які забезпечують надання життєво важливих послуг*** за визначеними Директивою секторами та підсекторами КІ. Єврокомісія, у співпраці з державами – членами ЄС, розробляє методики ідентифікації операторів КІ, які мають рекомендаційний характер.

Ідентифікація операторів КІ здійснюється визначеними уповноваженими державними органами держав-членів (*competent authorities*) на основі проведеного аналізу ризиків, стратегій держав – членів ЄС з урахуванням таких аспектів:

- оператор КІ забезпечує надання однієї або кількох життєво важливих послуг / функцій;

---

[3] Оцінка ризику – процес визначення характеру й масштабу ризику завдяки виявленню та аналізу потенційних загроз, уразливостей і небезпек, які можуть призвести до інциденту, а також потенційних втрат або збоїв у наданні основної послуги, спричинених цим інцидентом.

[4] Natural and man-made risks, including those of a cross-sectoral or cross-border nature, accidents, natural disasters, public health emergencies and hybrid threats or other antagonistic threats, including terrorist offences as provided for in Directive (EU) 2017/541 of the European Parliament and of the Council.

[5] The general risk assessment carried out pursuant to Article 6(1) of Decision No 1313/2013/EU; other relevant risk assessments, carried out in accordance with the requirements of the relevant sector-specific Union legal acts, including Directive (EU) 2017/541, Regulations (EU) 2017/1938, and (EU) 2019/941**,** Directives 2007/60/EC and 2012/18/EU.

- оператор КІ управляє КІ, розміщеною на території держави – члена ЄС;
- інцидент порушення функціонування КІ[6] може мати суттєвий негативний вплив на надання однієї або кількох життєво важливих послуг / функцій (визначених окремою державою) або надання послуг / функцій у визначених Директивою секторах.

Кожна з держав ЄС має оприлюднити національний перелік операторів КІ, повідомити призначених операторів, що вони увійшли до такого переліку та зобов'язані виконувати вимоги Директиви. Кожна держава має щонайменше раз на чотири роки переглядати перелік операторів КІ. Якщо за результатами перегляду оператор не відповідає встановленим критеріям, такий оператор КІ вилучається з переліку, а держава зобов'язана повідомити його в установлений строк про те, що він більше не відповідає вимогам Директиви CER.

6. Для створення єдиних методичних підходів щодо аналізу ризиків Директива наводить ***критерії оцінки суттєвого негативного ефекту*** (*significant disruptive effect*) впливу загроз на стійкість роботи оператора КІ, а саме:

- кількість користувачів, які покладаються на основні послуги, що надаються відповідним суб'єктом;
- ступінь, у якому інші сектори та підсектори, зазначені в Додатку до Директиви, залежать від відповідної основної послуги;
- вплив, який інциденти можуть мати, з точки зору ступеня та тривалості, на економічну та суспільну діяльність, довкілля, громадську безпеку, здоров'я населення;
- ринкова частка суб'єкта господарювання на ринку відповідної основної послуги або основних послуг;
- географічна територія, яка може постраждати від інциденту, включно з будь-яким транскордонним впливом, з урахуванням уразливості, пов'язаної зі ступенем ізоляції певних типів географічних територій, як-от острівні, віддалені або гірські райони;
- важливість суб'єкта в підтримці необхідного рівня основних послуг з урахуванням наявності альтернативних засобів для надання таких основних послуг.

Єврокомісія, після консультацій із Групою стійкості операторів КІ (*the Critical Entities Resilience Group*), розробляє із застосуванням зазначених критеріїв методики оцінювання суттєвого негативного ефекту, які мають рекомендаційний характер.

7. Після ідентифікації операторів КІ кожна з держав ЄС має надати Єврокомісії таку інформацію:

- перелік додаткових основних послуг в цій державі – члені ЄС порівняно зі списком основних послуг, наведених у Додатку до Директиви;
- кількість операторів КІ, визначених для кожного сектору й підсектору КІ та для кожної основної послуги;
- будь-які порогові значення, застосовані для визначення одного або кількох наведених критеріїв.

8. Операторам КІ держави надають підтримку щодо підвищення їхньої стійкості. Такою підтримкою може бути підготовка методичних та інструктивних матеріалів, допомога в організації та проведенні колективних навчань, консультування, запровадження програм підвищення кваліфікації персоналу операторів КІ. Держави

[6] «Інцидент» означає подію, яка потенційно може суттєво порушити або порушує надання основних послуг, у тому числі коли це впливає на національні системи, котрі захищають верховенство права.

сприяють добровільному обміну інформацією щодо завдань, визначених Директивою. Держави також можуть надавати фінансову допомогу операторам КІ для виконання вимог Директиви, якщо це необхідно і обґрунтовано суспільними інтересами.

9. Директива CER зобов'язує кожну державу – члена ЄС визначити ***одного або кількох уповноважених органів державної влади*** (the competent authority), відповідальних за виконання Директиви та встановлення правил регулювання діяльності в цій сфері на національному рівні. У випадку, коли держави оберуть не одного, а більше уповноважених органів влади, потрібно чітко окреслити завдання кожного з них, забезпечити їхню ефективну координацію та взаємодію при виконанні завдань Директиви.

Кожна держава – член ЄС інформує Єврокомісію про уповноважені органи, їхні завдання та відповідальність за виконання Директиви, а також способи комунікації. Держави ЄС забезпечують належну взаємодію та обмін інформацією уповноважених органів з відповідними інституціями щодо реагування на різні типи загроз.

При цьому кожна держава визначає уповноважений орган, який виконуватиме роль «єдиної точки контакту» (*single point of contact*) для транскордонної взаємодії, сприятиме співпраці держави з Групою стійкості операторів КІ, Єврокомісією, а також із третіми державами.

Визначена «точкою контакту» інституція подає до Єврокомісії та Групи стійкості операторів КІ звіт щодо інцидентів безпеки та заходів реагування на них згідно з вимогами Директиви. Єврокомісія разом із Групою стійкості операторів КІ розробляє єдиний для всіх держав ЄС шаблон звіту.

10. Відповідно до Директиви, між державами ЄС проводяться консультації щодо належної імплементації встановлених вимог. Зокрема предметом консультацій є робота операторів, які: використовують КІ, що фізично пов'язує дві або більше держав ЄС; є частиною корпоративної структури, що поєднана чи пов'язана з операторами КІ в інших державах; ідентифіковані як оператори КІ в одній з цих держав і забезпечують надання життєво важливих послуг / функцій в цій або в іншій державі.

11. Директива CER приділяє суттєву увагу ***діям операторів КІ щодо забезпечення їхньої стійкості***. Держави ЄС мають забезпечити проведення операторами КІ аналізу ризиків протягом дев'яти місяців з дати отримання повідомлення про включення їх до національного переліку.

У рамках аналізу ризиків оператор КІ оцінює вплив загроз усіх видів, враховує залежність інших секторів КІ (визначених Директивою) від послуг / функцій, що забезпечуються цим оператором КІ, а також залежність роботи цього оператора КІ від функцій / послуг, що надаються операторами в інших секторах та в інших державах.

Директива зобов'язує держави ЄС гарантувати застосування операторами КІ належних та адекватних рівню загроз технічних, безпекових та організаційних заходів забезпечення стійкості КІ, зокрема необхідних для:

- запобігання виникненню інцидентів, ураховуючи заходи адаптації до зміни клімату та зменшення впливу природних катастроф;
- забезпечення належного фізичного захисту приміщень та інфраструктури, наприклад, огорожі, бар'єри, інструменти та процедури моніторингу периметра, обладнання виявлення та контролю доступу;

- реагування на інциденти, протистояння їм і пом'якшення їхніх наслідків, ураховуючи впровадження процедур і протоколів управління ризиками та кризовими ситуаціями, а також оповіщення;
- відновлення після інцидентів, ураховуючи заходи забезпечення безперервності бізнесу та визначення альтернативних ланцюгів постачання, щоб поновити надання основних послуг;
- адекватного управління безпекою працівників, ураховуючи такі заходи, як визначення категорій персоналу, що виконує критично важливі функції, встановлення прав доступу до приміщень, об'єктів КІ та конфіденційної інформації, встановлення процедур для перевірки даних і визначення категорій осіб, які повинні проходити такі перевірки, встановлення відповідних вимог до підготовки та кваліфікації;
- підвищення обізнаності персоналу, враховуючи навчальні курси, інформаційні матеріали та навчання.

12. Держави ЄС мають забезпечити ***застосування операторами КІ планів стійкості***, які охоплюють вищенаведені заходи. У процесі моніторингу виконання операторами КІ вимог Директиви уповноважені органи держав ЄС визначають адекватність та відповідність таких планів установленим вимогам. Для взаємодії та обміну інформацією оператори КІ мають призначити посадову особу в ролі «точки контакту».

13. Директива запроваджує низку інструментів ***моніторингу готовності та стійкості операторів КІ до реалізації загроз порушення життєво важливих функцій / послуг.***

Одним із таких інструментів є організація Єврокомісією ***консультативних місій*** (*advisory missions*) для надання рекомендацій операторам КІ щодо виконання положень Директиви. Результати роботи направлених до оператора КІ консультативних місій оформлюються у звіті та надаються оператору КІ, відповідній державі ЄС та Єврокомісії. Єврокомісія, після консультацій з Групою стійкості операторів КІ, формує методичні рекомендації щодо деталізації проведення місій та підготовки заходів забезпечення стійкості операторів КІ.

Іншим інструментом підвищення стійкості операторів КІ є запровадження практики ***перевірки персоналу*** (*background checks*). Держави ЄС мають визначити умови, за яких операторам КІ дозволяється, в обгрунтованих випадках, подавати запит щодо перевірки інформації стосовно особи, яка:

- обіймає важливу посаду, виконує критичну роль у штаті оператора КІ або на його користь, зокрема щодо забезпечення стійкості оператора КІ;
- має право прямого або віддаленого доступу до приміщень, інформації чи систем управління, пов'язаних з питаннями безпеки оператора КІ;
- розглядається для призначення на посаду, яка відповідає зазначеним критеріям.

Такі перевірки матимуть обмежений характер, проводитимуться виключно за нагальної необхідності та лише з точки зору аналізу ризиків безпеці оператора КІ.

14. Держави ЄС мають забезпечити ***інформування операторами КІ уповноважених органів*** (*submit an initial notification*) щодо інцидентів, які потенційно можуть суттєво порушити надання життєво важливих функцій / послуг. Інформування здійснюється протягом 24 годин з моменту ідентифікації такого інциденту з наступною підготовкою та поданням детального звіту протягом одного місяця. Аналізуючи ці випадки, потрібно враховувати такі параметри:

- кількість і частку користувачів, які постраждали від збою;
- тривалість переривання надання послуг;
- географічну територію, що постраждала від руйнування, з урахуванням того, чи є ця територія географічно ізольованою.

Якщо інцидент може призвести до порушення надання життєво важливих функцій / послуг у шести або більше державах – членах ЄС, уповноважений орган держави, де відбувся інцидент, має поінформувати про це Єврокомісію. Таке повідомлення має містити інформацію щодо характеру, причини та можливих наслідків інциденту, включно з будь-якими іншими відомостями, необхідними для визначення будь-якого транскордонного впливу.

Уповноважений орган держави, де відбувся інцидент, через «точку контакту» має також поінформувати уповноважені органи держав, на які може вплинути цей інцидент. Після отримання відповідної інформації уповноважений орган іншої держави має якнайшвидше повідомити відповідних операторів КІ про потенційні загрози для підтримання їхньої готовності належним чином реагувати на загрози.

15. Директива окремо визначає ***особливості застосування вимог до операторів КІ загальноєвропейського значення***. Віднесення до операторів КІ загальноєвропейського значення (*critical entity of particular European significance*), здійснюється, коли оператор КІ:

- ідентифікований як оператор КІ державою ЄС та був повідомлений про його внесення до національного переліку операторів КІ;
- забезпечує надання життєво важливих функцій / послуг для шести і більше держав ЄС.

Держави мають визначити процедури повідомлення уповноваженим органом оператора КІ, що він забезпечує надання послуг для шести і більше держав ЄС, а також інших держав ЄС щодо такого оператора. Держави мають також поінформувати Єврокомісію щодо ідентифікації такого оператора КІ.

У рамках консультацій Єврокомісії з уповноваженим органом держави ЄС, у якій ідентифіковано оператора КІ загальноєвропейського значення, уточнюється, чи є послуги, які надає такий оператор, життєво важливими для ЄС. У разі визнання Єврокомісією поданого їй оператора КІ оператором КІ загальноєвропейського значення, про таке рішення йому повідомляє уповноважений орган держави – члена ЄС. Вимоги до особливостей застосування Директиви CER для таких операторів активуються в момент отримання оператором повідомлення про його визначення оператором КІ загальноєвропейського значення.

На запит держави-члена Єврокомісія організовує консультативну місію для оцінки заходів, які запровадив оператор КІ загальноєвропейського значення для виконання своїх зобов'язань згідно з вимогами Директиви.

Консультативна місія повідомляє про свої висновки Єврокомісію та відповідну державу щодо результатів оцінки протягом трьох місяців після завершення місії.

Єврокомісія, ґрунтуючись на результатах роботи місії, повідомляє свою думку відповідній державі ЄС та оператору КІ щодо того, чи виконуються ними заходи, які можуть бути вжиті для підвищення стійкості роботи такого оператора КІ. Держава – член ЄС має забезпечити, щоб її уповноважений орган і відповідний оператор КІ враховували надані рекомендації та поінформували Єврокомісію та держав-членів, яким або в яких надається життєво важлива послуга / функція, про заходи, що їх було вжито відповідно до такого висновку.

Єврокомісія приймає імплементаційний акт, що встановлює процедури ініціювання, проведення та розгляду звіту консультативної місії. При цьому держави – члени ЄС мають гарантувати, що оператори КІ загальноєвропейського значення нададуть консультативним місіям необхідний доступ до інформації, систем і засобів, котрі стосуються надання їхніх основних послуг.

Єврокомісія також інформує Групу стійкості операторів КІ щодо організації консультативної місії, а також про основні результати її роботи з метою взаємного навчання та поширення кращого досвіду.

16. Директива запроваджує ***механізм обміну інформацією та кращим досвідом серед держав ЄС***, операторів КІ та інших залучених інституцій. Зокрема створюється Група стійкості операторів КІ, яка має підтримувати Єврокомісію, сприяти співпраці між державами – членами ЄС та обміну інформацією з питань стійкості надання життєво важливих послуг / функцій.

Відповідно до Директиви, Група має складатися з представників Єврокомісії і держав-членів, які мають дозвіл з питань безпеки (якщо це необхідно). За потреби можуть запрошуватися інші зацікавлені сторони. Очолює Групу представник Єврокомісії. Комісія може приймати імплементаційні акти, що встановлюють процедурні механізми, необхідні для функціонування Групи. Кожні два роки Група розробляє робочу програму дій, які необхідно вжити для реалізації її цілей і завдань.

Завданнями Групи стійкості операторів КІ, зокрема, є:

- підтримка Єврокомісії в наданні державам-членам допомоги у зміцненні їхньої спроможності сприяти стійкості операторів КІ;
- аналіз стратегій держав ЄС;
- допомога в обміні найкращими практиками стосовно ідентифікації операторів КІ державами-членами, зокрема щодо транскордонних і міжгалузевих залежностей, а також ризиків та інцидентів;
- сприяння підготовці методичних рекомендацій та, на запит, будь-яких делегованих або імплементаційних актів, ухвалених відповідно до Директиви;
- аналіз підсумкових звітів держав-членів, обмін інформацією та найкращими практиками щодо повідомлення про інциденти, інновацій, досліджень і розробок, пов’язаних зі стійкістю КІ;
- обговорення підсумкових звітів консультативних місій та отриманих результатів;
- обмін інформацією з питань, що стосуються стійкості операторів КІ, з відповідними інституціями, органами, службами та агентствами ЄС.

Згідно з Директивою, Єврокомісія має підтримувати держави-члени та операторів КІ у виконанні їхніх зобов’язань. Комісія готує на рівні ЄС огляд транскордонних і міжгалузевих ризиків для надання основних послуг, організовує консультативні місії, сприяє обміну інформацією між державами-членами та експертами. Комісія доповнює діяльність держав-членів розробленням найкращих практик, керівних матеріалів і методологій, а також транскордонними навчальними заходами з метою перевірки стійкості операторів КІ. Комісія також інформує держави-члени про фінансові ресурси на рівні Союзу, доступні державам-членам для виконання Директиви.

17. Директива запроваджує механізм моніторингу її виконання. Для оцінки відповідності операторів КІ зобов’язанням, викладеним у Директиві, держави-члени мають надати уповноваженим органам повноваження та засоби для проведення

інспекції об’єктів КІ та приміщень, які оператор КІ використовує для надання своїх основних послуг, а також для здійснення дистанційного нагляду за вжитими оператором заходами.

18. Держави-члени мають надати уповноваженим органам повноваження та засоби вимагати від операторів КІ:

- інформацію, необхідну для оцінки того, чи відповідають заходи, вжиті цими операторами для забезпечення їхньої стійкості, вимогам Директиви;
- докази ефективного впровадження таких заходів, включно з результатами аудиту, проведеного незалежним і кваліфікованим аудитором, обраним оператором та здійсненим за його рахунок.

Запитуючи такі відомості, уповноважені органи мають зазначити мету проведення перевірки та інформацію, яку очікують отримати від оператора КІ.

Директива передбачає, що у випадку порушення зобов’язань ***до операторів КІ можуть застосовуватися санкції***. Держави – члени ЄС мають встановити правила щодо санкцій, які застосовуються у разі порушень національних заходів, визначених відповідно до Директиви, і забезпечити їх виконання. Такі санкції мають бути ефективними, пропорційними та переконливими. Держави-члени мають повідомляти Єврокомісію про зазначені правила та заходи, а також про будь-які їх зміни.

Відповідно до Директиви, держава – член ЄС має забезпечити, що повноваження уповноважених органів та їх застосування до операторів КІ, здійснюватимуться лише за умови відповідних гарантій і відбуватимуться в об’єктивний, прозорий і пропорційний спосіб, а права та законні інтереси (наприклад, захист комерційної таємниці) суб’єктів, яких це стосується, будуть належним чином захищені, включно з правом бути почутим і правом на ефективний правовий захист у незалежному суді.