Аналіз регуляторного впливу
до проєкту наказу Міністерства енергетики України
«Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж»

І. Визначення проблеми

Проєкт наказу «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж» (далі – проєкт наказу) розроблено Міністерством енергетики України відповідно до пункту 2 Плану заходів щодо реалізації Концепції впровадження «розумних мереж» в Україні до 2035 року, затвердженого розпорядженням Кабінету Міністрів України від 14.10.2022 № 908-р, з урахуванням доручень Прем'єр-міністра України Дениса ШМИГАЛЯ від 28.03.2024 № 40517/8/1-23 та заступника Державного секретаря Кабінету Міністрів Олега ВОЙТОВИЧА від 05.04.2024 № 8260/0/2-24.

Постановою Кабінету Міністрів України від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури» Міненерго визначено уповноваженим органом державної влади, відповідальним за паливно-енергетичний сектор критичної інфраструктури.

Наказом Міненерго від 07.09.2022 № 1-ДСК (зі змінами) затверджено Перелік об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури.

Наказом Міненерго від 16.12.2022 № 5-ДСК (зі змінами) затверджено Перелік об'єктів критичної інформаційної інфраструктури паливно-енергетичного сектору критичної інфраструктури.

Відповідно до пункту 7 частини четвертої статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури, є суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки.

Одним з основних чинників, що створює небезпеку об'єктам критичної інфраструктури є кіберзагрози та кібератаки.

24.02.2022 російська федерація розпочала військову агресію проти держави Україна. У зв'язку з цим, відповідно до Указу Президента України від 24.02.2022 № 64/2022 в Україні введено воєнний стан, строк дії якого продовжено. російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно об'єктів критичної інфраструктури, в тому числі електричних мереж.

Розроблення проєкту наказу зумовлено необхідністю оцінки та вдосконалення програм з кібербезпеки електричних мереж та зміцнення їх експлуатаційної стійкості, покращення стану кібербезпеки електричних мереж, ння їх захищеності.

Під час визначення проблеми, яку передбачається розв’язати шляхом державного регулювання, встановлені основні групи, на які проблема справляє вплив:

Групи (підгрупи)	Так	Ні
Громадяни	-	+
Держава	+	-
Суб’єкти господарювання	+	-

Ця проблема не може бути вирішена за допомогою ринкових механізмів, оскільки визначення моделі зрілості спроможностей кібербезпеки електричних мереж, індикаторів та індексів стану кібербезпеки електричних мереж можливе лише за допомогою державного регулювання.

II. Цілі державного регулювання

Основною ціллю проєкту наказу є затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж, що визначає модель зрілості спроможностей кібербезпеки електричних мереж, яка базується на моделі зрілості спроможностей кібербезпеки Cybersecurity capability maturity model program (C2M2). Модель C2M2 призначена для використання операторами критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури з метою здійснення самооцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж, як об’єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	Залишення існуючої ситуації без змін. Відсутність об’єктивної інформації щодо оцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж, як об’єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури, в цілому призведе до збільшення ризиків порушення стабільного функціонування електричних мереж внаслідок кібератак.
Альтернатива 2	Прийняття проєкту наказу. Прийняття проєкту наказу забезпечить досягнення вищезгаданих цілей державного регулювання повною мірою.

2. Оцінка обраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні.	Відсутність нормативно-правової бази щодо оцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж. Збереження існуючої ситуації збільшує ризик значних матеріальних збитків внаслідок масштабних кібератак.
Альтернатива 2	Прийняття проєкту наказу забезпечить: - виконання пункту 2 Плану заходів щодо реалізації Концепції впровадження «розумних мереж» в Україні до 2035 року, затвердженого розпорядженням Кабінету Міністрів України від 14.10.2022 № 908-р, з урахуванням доручень Прем'єр-міністра України Дениса ШМИГАЛЯ від 28.03.2024 № 40517/8/1-23 та заступника Державного секретаря Кабінету Міністрів Олега ВОЙТОВИЧА від 05.04.2024 № 8260/0/2-24; - оцінку та вдосконалення програми з кібербезпеки електричних мереж; - зміцнення кіберстійкості та покращення стану кібербезпеки електричних мереж. Це дозволить об'єктивно оцінити реальний стан кібербезпеки електричних мереж з урахуванням реальних і потенційних загроз у кіберпросторі та визначити напрями	Відсутні.

	вдосконалення і розвитку системи кібербезпеки електричних мереж, що в свою чергу забезпечить можливість суттєвого зменшення імовірності виникнення аварійних ситуацій та аварій (спричинених кібератаками) з вкрай негативними наслідками для держави, населення та навколишнього природного середовища.	

Оцінка впливу на громадян не проводилась, оскільки положення проєкту наказу на них не поширюються.

Оцінка впливу на сферу інтересів суб'єктів господарювання (операторів критичної інфраструктури) *

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання (одиниць)	69	66	-	-	135
Питома вага групи у загальній кількості, відсотків	51,1	48,9	-	-	100

* Відповідно до Переліку об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури, затвердженого наказом Міністерства енергетики України від 07.09.2022 № 1-ДСК (зі змінами).

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні.	Негативний вплив на безпеку електричних мереж через ризик виникнення аварійних ситуацій або аварій внаслідок можливих кібератак. Виникнення аварійних ситуацій через кібератаки може призвести до значних матеріальних збитків. Виникнення аварій через

		кібератаки може призвести до забруднення навколишнього природного середовища, нанесення шкоди здоров'ю персоналу та населенню, значних витрат на ліквідацію наслідків аварії.
Альтернатива 2	Покращення стану кібербезпеки електричних мереж завдяки реалізації програм з удосконалення кібербезпеки. Зменшення імовірності виникнення аварійних ситуацій наслідок кібератак. Забезпечення стабільно безпечної та економічно ефективної роботи електричних мереж.	Відсутні.

Витрати на одного суб'єкта господарювання великого підприємництва і середнього підприємництва, які виникають внаслідок дії регуляторного акта (згідно з додатком 2 до Методики проведення аналізу впливу регуляторного акта).

Порядковий номер	Витрати	За перший рік	За п'ять років
1	Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання/підвищення кваліфікації персоналу тощо, гривень.	0,00	0,00
2	Податки та збори (зміна розміру податків/зборів, виникнення необхідності у сплаті податків/зборів), гривень.	0,00	0,00
3	Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам, гривень.	3000,00	5000,00
4	Витрати, пов'язані з адмініструванням заходів	0,00	0,00

	державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/ приписів тощо), гривень.		
5	Витрати на отримання адміністративних послуг (дозволів, ліцензій, сертифікатів, атестатів, погоджень, висновків, проведення незалежних/обов'язкових експертиз, сертифікації, атестації тощо) та інших послуг (проведення наукових, інших експертиз, страхування тощо), гривень.	0,00	0,00
6	Витрати на оборотні активи (матеріали, канцелярські товари тощо), гривень.	200,00	1000,00
7	Витрати, пов'язані із наймом додаткового персоналу, гривень.	0,00	0,00
8	Інше (уточнити), гривень.	0,00	0,00
9	РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8), гривень.	3200,00	6000,00
10	Кількість суб'єктів господарювання великого та середнього підприємництва, на яких буде поширено регулювання, одиниць.	135	135
11	Сумарні витрати суб'єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 9 х рядок 10), гривень.	432000,00	810000,00

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1	Надвеликі витрати на ліквідацію наслідків аварій в електричних

	мережах.
Альтернатива 2	810000,00

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1	1	Цілі регулювання не можуть бути досягнуті (проблема продовжить існувати).
Альтернатива 2	4	Прийняття проєкту наказу забезпечить повною мірою досягнення поставлених цілей.

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1	Відсутні.	Відсутність нормативно-правової бази щодо оцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж призводить до відсутності об’єктивної інформації щодо оцінки рівня кібербезпеки електричних мереж, як наслідок, до вразливості об’єктів критичної інфраструктури у кіберпросторі. Збереження існуючої ситуації збільшує ризик значних	Альтернатива не забезпечує досягнення цілей регулювання. За відсутності вигод, кількість неврегульованих витрат залишається значною.

		матеріальних збитків внаслідок кібератак. Негативний вплив на безпеку електричних мереж через ризик виникнення аварійних ситуацій або аварій внаслідок можливих кібератак, спрямованих на електричні мережі.	
Альтернатива 2	Прийняття проєкту наказу забезпечить: - затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж; - визначення: моделі зрілості спроможностей кібербезпеки електричних мереж, як об'єктів критичної інфраструктури; індикаторів та індексів стану кібербезпеки електричних мереж; - проведення самооцінки стану кіберзахисту електричних мереж; - отримання об'єктивної та повної оцінки рівня кібербезпеки електричних мереж, як об'єктів критичної інфраструктури. - формування пропозицій щодо вдосконалення законодавства у	Відсутні.	Альтернатива забезпечує досягнення цілей регулювання. За відсутності витрат, дозволяє досягнути максимальної кількості вигод.

	сфері кібербезпеки, кіберзахисту та визначення напрямів розвитку системи кібербезпеки паливно-енергетичного сектору критичної інфраструктури в частині кіберзахисту; - планування заходів щодо забезпечення кіберстійкості електричних мереж. Це призведе до визначення напрямів вдосконалення і розвитку електричних мереж, що суттєво зменшить імовірність виникнення аварійних ситуацій та аварій (спричинених кібератаками) з вкрай негативними наслідками для держави, населення та навколишнього природного середовища.		

V. Механізми та заходи, які забезпечать розв’язання визначеної проблеми

Механізмами, що забезпечать розв’язання визначеної проблеми, є прийняття проєкту наказу.

Проєктом наказу пропонується: затвердити Методику оцінювання стану кібербезпеки електричних мереж; практики кібербезпеки електричних мереж.

Організаційні заходи, які необхідно здійснити Міністерству енергетики України для впровадження наказу «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж»:

- направлення операторам критичної інфраструктури інформаційних листів щодо набрання чинності регуляторним актом;

- розміщення на сайті Міністерства енергетики України www.mev.gov.ua наказу «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж»;

- проведення операторами критичної інфраструктури самооцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж, як об'єктів критичної інфраструктури;

- підготовка звітів за результатами застосування моделі C2M2, що надсилаються операторам критичної інфраструктури до Міненерго.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

Реалізація регуляторного акта не потребуватиме додаткових бюджетних витрат і ресурсів на адміністрування регулювання органами виконавчої влади чи органами місцевого самоврядування.

М-тест не проводився оскільки малі суб'єкти господарювання не зазнають витрат на впровадження регуляторного акта.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Регуляторний акт набирає чинності з дня його офіційного опублікування.

Строк дії цього регуляторного акта не обмежується у часі, що надасть можливість розв'язати проблеми та досягти цілей державного регулювання.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозними значеннями показників результативності регуляторного акта є:

- розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов'язаних з дією акта – не передбачається;

- кількість суб'єктів господарювання, на яких поширюється дія акта: 135 суб'єктів господарювання (операторів критичної інфраструктури), які підпадають під дію регулювання регуляторного акта;

- розмір коштів і час, що витрачатимуться органами виконавчої влади, пов'язаними з виконанням вимог акта – не змінюється (в межах робочого часу працівників та коштів, передбачених на фінансування заробітної плати для них);

- рівень поінформованості суб'єктів господарювання з основних положень акта – середній. Проєкт акта розміщено на веб-сайті Міністерства енергетики України www.mev.gov.ua, а після прийняття акта він буде розміщений на сайті www.zakon.rada.gov.ua.

- кількість скарг/звернень громадян/суб'єктів господарювання, пов'язаних із дією регуляторного акта;

- кількість погоджених документів;

- кількість виявлених порушень, пов'язаних із дією акта.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Базове відстеження результативності регуляторного акта здійснюється після набрання чинності цим регуляторним актом, але не пізніше дня, з якого починається проведення повторного відстеження результативності цього акта.

Повторне відстеження результативності регуляторного акта здійснюється через 1 рік з дня набрання ним чинності.

Періодичні відстеження результативності регуляторного акта здійснюються раз на кожні три роки починаючи з дня закінчення заходів з повторного відстеження результативності цього акта.

Міністр енергетики України **Герман ГАЛУЩЕНКО**

«___» _____ 2024 року

Додаток
до Методики оцінювання
стану кібербезпеки
електричних мереж

Індикатори та індекси
стану кібербезпеки електричних мереж

1. Модель C2M2 використовує 4 рівні MIL для визначення подвійного прогресу зрілості (прогресу підходу та прогресу управління).

2. Значення MIL мають діапазон від MIL0 до MIL3 і призначені для незалежного застосування до кожної області:

1) MIL0 – практики не виконуються;

2) MIL1 – початкові практики виконуються, але можуть бути ситуативними;

3) MIL2 – дії документуються. Дії та ініціативи забезпечені належними ресурсами і при впровадженні керуються стандартами та керівними принципами;

4) MIL3 – управління та політики кібербезпеки спрямовують дії, визначено вимоги відповідності, виконуються перевірки для забезпечення відповідності вимогам, визначені відповідальність, підзвітність та повноваження персоналу оператора, у якого також є належні навички та знання у сфері кібербезпеки.

3. Кожна з практик має один рівень MIL з наявних чотирьох (від MIL0 до MIL3).

4. Аспекти рівнів MIL, що є важливими для розуміння та застосування моделі C2M2:

1) рівні MIL застосовуються незалежно до кожної області. У результаті оператор, який використовує модель C2M2, може працювати з різними рейтингами MIL у різних областях;

2) індекси MIL (від MIL0 до MIL3) накопичуються в кожній області. Щоб отримати MIL у певній області, оператор повинен виконати всі практики на поточному рівні MIL та на попередньому рівні MIL;

3) в інструментах самооцінки моделі C2M2 практика вважається виконаною, якщо вибрано відповідь LI або FI.

5. Визначення рівня MIL в області ASSET:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області ASSET рівень впровадження кожної з практик ASSET-1a, ASSET-2a, ASSET-3a, ASSET-4a, ASSET-4b області ASSET за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області ASSET рівень впровадження кожної практик ASSET-1a, ASSET-2a, ASSET-3a, ASSET-4a, ASSET-4b, ASSET-1b, ASSET-1c, ASSET-1d, ASSET-1e, ASSET-2b, ASSET-2c, ASSET-2d, ASSET-2e, ASSET-3b, ASSET-3c, ASSET-3d, ASSET-4c, ASSET-4d, ASSET-4e, ASSET-4f, ASSET-4g, ASSET-5a, ASSET-5b області ASSET за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області ASSET рівень впровадження кожної з практик ASSET-1a, ASSET-2a, ASSET-3a, ASSET-4a, ASSET-4b, ASSET-1b, ASSET-1c, ASSET-1d, ASSET-1e, ASSET-2b, ASSET-2c, ASSET-2d, ASSET-2e, ASSET-3b, ASSET-3c, ASSET-3d, ASSET-4c, ASSET-4d, ASSET-4e, ASSET-4f, ASSET-4g, ASSET-5a, ASSET-5b, ASSET-1f, ASSET-1g, ASSET-1h, ASSET-2f, ASSET-2g, ASSET-2h, ASSET-3e, ASSET-4h, ASSET-4i, ASSET-5c, ASSET-5d, ASSET-5e, ASSET-5f області ASSET за чотирьохбальною шкалою має бути LI або FI;

6. Визначення рівня MIL в області THREAT:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області THREAT рівень впровадження кожної з практик THREAT-1a, THREAT-1b, THREAT-1c, THREAT-1d, THREAT-2a, THREAT-2b, THREAT-2c, THREAT-2d області THREAT за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області THREAT рівень впровадження кожної з практик THREAT-1a, THREAT-1b, THREAT-1c, THREAT-1d, THREAT-2a, THREAT-2b, THREAT-2c, THREAT-2d, THREAT-1e, THREAT-1f, THREAT-1g, THREAT-1h, THREAT-1i, THREAT-2e, THREAT-2f, THREAT-2g, THREAT-2h, THREAT-3a, THREAT-3b області THREAT за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області THREAT рівень впровадження кожної з практик THREAT-1a, THREAT-1b, THREAT-1c, THREAT-1d, THREAT-2a, THREAT-2b, THREAT-2c, THREAT-2d, THREAT-1e, THREAT-1f, THREAT-1g, THREAT-1h, THREAT-1i, THREAT-2e,

THREAT-2f, THREAT-2g, THREAT-2h, THREAT-3a, THREAT-3b, THREAT-1j, THREAT-1k, THREAT-1l, THREAT-1m, THREAT-2i, THREAT-2j, THREAT-2k, THREAT-3c, THREAT-3d, THREAT-3e, THREAT-3f області THREAT за чотирьохбальною шкалою має бути LI або FI.

7. Визначення рівня MIL в області RISK:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області RISK рівень впровадження кожної з практик RISK-1a, RISK-2a, RISK-3a, RISK-4a області RISK за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області RISK рівень впровадження кожної з практик RISK-1a, RISK-2a, RISK-3a, RISK-4a, RISK-1b, RISK-1c, RISK-1d, RISK-1e, RISK-1f, RISK-2b, RISK-2c, RISK-2d, RISK-2e, RISK-2f, RISK-2g, RISK-3b, RISK-3c, RISK-3d, RISK-3e, RISK-3f, RISK-4b, RISK-5a, RISK-5b області RISK за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області RISK рівень впровадження кожної з практик RISK-1a, RISK-2a, RISK-3a, RISK-4a, RISK-1b, RISK-1c, RISK-1d, RISK-1e, RISK-1f, RISK-2b, RISK-2c, RISK-2d, RISK-2e, RISK-2f, RISK-2g, RISK-3b, RISK-3c, RISK-3d, RISK-3e, RISK-3f, RISK-4b, RISK-5a, RISK-5b, RISK-1g, RISK-1h, RISK-2h, RISK-2i, RISK-2j, RISK-2k, RISK-2l, RISK-2m, RISK-3g, RISK-4c, RISK-4d, RISK-4e, RISK-5c, RISK-5d, RISK-5e, RISK-5f області RISK за чотирьохбальною шкалою має бути LI або FI;

8. Визначення рівня MIL в області ACCESS:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області ACCESS рівень впровадження кожної з практик ACCESS-1a, ACCESS-1b, ACCESS-1c, ACCESS-2a, ACCESS-2b, ACCESS-3a, ACCESS-3b, ACCESS-3c області ACCESS за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області ACCESS рівень впровадження кожної з практик ACCESS-1a, ACCESS-1b, ACCESS-1c, ACCESS-2a, ACCESS-2b, ACCESS-3a, ACCESS-3b, ACCESS-3c, ACCESS-1d, ACCESS-1e, ACCESS-1f, ACCESS-1g, ACCESS-1h, ACCESS-2c, ACCESS-2d, ACCESS-2e, ACCESS-2f, ACCESS-2g, ACCESS-3d, ACCESS-3e, ACCESS-3f, ACCESS-3g, ACCESS-3h, ACCESS-4a, ACCESS-4b області ACCESS за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області ACCESS рівень впровадження кожної з практик ACCESS-1a, ACCESS-1b,

ACCESS-1c, ACCESS-2a, ACCESS-2b, ACCESS-3a, ACCESS-3b, ACCESS-3c, ACCESS-1d, ACCESS-1e, ACCESS-1f, ACCESS-1g, ACCESS-1h, ACCESS-2c, ACCESS-2d, ACCESS-2e, ACCESS-2f, ACCESS-2g, ACCESS-3d, ACCESS-3e, ACCESS-3f, ACCESS-3g, ACCESS-3h, ACCESS-4a, ACCESS-4b, ACCESS-1i, ACCESS-1j, ACCESS-2h, ACCESS-2i, ACCESS-3i, ACCESS-3j, ACCESS-4c, ACCESS-4d, ACCESS-4e, ACCESS-4f області ACCESS за чотирьохбальною шкалою має бути LI або FI.

9. Визначення рівня MIL в області SITUATION:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області SITUATION рівень впровадження кожної з практик SITUATION-1a, SITUATION-2a, SITUATION-2b області SITUATION за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області SITUATION рівень впровадження кожної з практик SITUATION-1a, SITUATION-2a, SITUATION-2b, SITUATION-1b, SITUATION-1c, SITUATION-1d, SITUATION-1e, SITUATION-2c, SITUATION-2d, SITUATION-2e, SITUATION-2f, SITUATION-3a, SITUATION-3b, SITUATION-3c, SITUATION-4a, SITUATION-4b області SITUATION за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області SITUATION рівень впровадження кожної з практик SITUATION-1a, SITUATION-2a, SITUATION-2b, SITUATION-1b, SITUATION-1c, SITUATION-1d, SITUATION-1e, SITUATION-2c, SITUATION-2d, SITUATION-2e,SITUATION-2f, SITUATION-3a, SITUATION-3b, SITUATION-3c, SITUATION-4a, SITUATION-4b, SITUATION-1f, SITUATION-2g, SITUATION-2h, SITUATION-2i, SITUATION-3d, SITUATION-3e, SITUATION-3f, SITUATION-3g, SITUATION-4c, SITUATION-4d, SITUATION-4e, SITUATION-4f області SITUATION за чотирьохбальною шкалою має бути LI або FI.

10. Визначення рівня MIL в області RESPONSE:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області RESPONSE рівень впровадження кожної з практик RESPONSE-1a, RESPONSE-2a, RESPONSE-2b, RESPONSE-3a, RESPONSE-3b, RESPONSE-3c, RESPONSE-4a, RESPONSE-4b, RESPONSE-4c області RESPONSE за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області RESPONSE рівень впровадження кожної з практик RESPONSE-1a,

RESPONSE-2a, RESPONSE-2b, RESPONSE-3a, RESPONSE-3b, RESPONSE-3c, RESPONSE-4a, RESPONSE-4b, RESPONSE-4c, RESPONSE-1b, RESPONSE-1c, RESPONSE-2c, RESPONSE-2d, RESPONSE-2e, RESPONSE-2f, RESPONSE-2g, RESPONSE-3d, RESPONSE-3e, RESPONSE-3f, RESPONSE-3g, RESPONSE-3h, RESPONSE-4d, RESPONSE-4e, RESPONSE-4f, RESPONSE-4g, RESPONSE-4h, RESPONSE-4i, RESPONSE-4j, RESPONSE-4k, RESPONSE-4l, RESPONSE-5a, RESPONSE-5b області RESPONSE за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області RESPONSE рівень впровадження кожної з практик RESPONSE-1a, RESPONSE-2a, RESPONSE-2b, RESPONSE-3a, RESPONSE-3b, RESPONSE-3c, RESPONSE-4a, RESPONSE-4b, RESPONSE-4c, RESPONSE-1b, RESPONSE-1c, RESPONSE-2c, RESPONSE-2d, RESPONSE-2e, RESPONSE-2f, RESPONSE-2g, RESPONSE-3d, RESPONSE-3e, RESPONSE-3f, RESPONSE-3g, RESPONSE-3h, RESPONSE-4d, RESPONSE-4e, RESPONSE-4f, RESPONSE-4g, RESPONSE-4h, RESPONSE-4i, RESPONSE-4j, RESPONSE-4k, RESPONSE-4l, RESPONSE-5a, RESPONSE-5b, RESPONSE-1d RESPONSE-1e RESPONSE-1f RESPONSE-2h RESPONSE-2i RESPONSE-3i RESPONSE-3j RESPONSE-3k RESPONSE-3l RESPONSE-4m RESPONSE-4n RESPONSE-4o RESPONSE-4p RESPONSE-5c RESPONSE-5d RESPONSE-5e RESPONSE-5f області RESPONSE за чотирьохбальною шкалою має бути LI або FI.

11. Визначення рівня MIL в області THIRD-PARTIES:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області THIRD-PARTIES рівень впровадження кожної з практик THIRD-PARTIES-1a, THIRD-PARTIES-1b, THIRD-PARTIES-2a, THIRD-PARTIES-2b області THIRD-PARTIES за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області THIRD-PARTIES рівень впровадження кожної з практик THIRD-PARTIES-1a, THIRD-PARTIES-1b, THIRD-PARTIES-2a, THIRD-PARTIES-2b, THIRD-PARTIES-1c, THIRD-PARTIES-1d, THIRD-PARTIES-1e, THIRD-PARTIES-2c, THIRD-PARTIES-2d, THIRD-PARTIES-2e, THIRD-PARTIES-2f, THIRD-PARTIES-2g, THIRD-PARTIES-3a, THIRD-PARTIES-3b області THIRD-PARTIES за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області THIRD-PARTIES рівень впровадження кожної з практик THIRD-PARTIES-1a, THIRD-PARTIES-1b, THIRD-PARTIES-2a, THIRD-PARTIES-2b, THIRD-PARTIES-1c THIRD-PARTIES-1d, THIRD-PARTIES-1e, THIRD-PARTIES-2c, THIRD-PARTIES-2d, THIRD-PARTIES-2e,

THIRD-PARTIES-2f, THIRD-PARTIES-2g, THIRD-PARTIES-3a, THIRD-PARTIES-3b, THIRD-PARTIES-1f, THIRD-PARTIES-2h, THIRD-PARTIES-2i, THIRD-PARTIES-2j, THIRD-PARTIES-2k, THIRD-PARTIES-2l, THIRD-PARTIES-2m, THIRD-PARTIES-3c, THIRD-PARTIES-3d, THIRD-PARTIES-3e, THIRD-PARTIES-3f області THIRD-PARTIES за чотирьохбальною шкалою має бути LI або FI.

12. Визначення рівня MIL в області WORKFORCE:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області WORKFORCE рівень впровадження кожної з практик WORKFORCE-1a, WORKFORCE-1b, WORKFORCE-2a, WORKFORCE-3a, WORKFORCE-3b, WORKFORCE-4a, WORKFORCE-4b області WORKFORCE за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області WORKFORCE рівень впровадження кожної з практик WORKFORCE-1a, WORKFORCE-1b, WORKFORCE-2a, WORKFORCE-3a, WORKFORCE-3b, WORKFORCE-4a, WORKFORCE-4b, WORKFORCE-1c, WORKFORCE-1d, WORKFORCE-1e, WORKFORCE-2b, WORKFORCE-2c, WORKFORCE-2d, WORKFORCE-3c, WORKFORCE-3d, WORKFORCE-4c, WORKFORCE-4d, WORKFORCE-5a, WORKFORCE-5b області WORKFORCE за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області WORKFORCE рівень впровадження кожної з практик WORKFORCE-1a, WORKFORCE-1b, WORKFORCE-2a, WORKFORCE-3a, WORKFORCE-3b, WORKFORCE-4a, WORKFORCE-4b, WORKFORCE-1c, WORKFORCE-1d, WORKFORCE-1e, WORKFORCE-2b, WORKFORCE-2c, WORKFORCE-2d, WORKFORCE-3c, WORKFORCE-3d, WORKFORCE-4c, WORKFORCE-4d, WORKFORCE-5a, WORKFORCE-5b, WORKFORCE-1f WORKFORCE-1g WORKFORCE-2e WORKFORCE-2f, WORKFORCE-2g, WORKFORCE-3e, WORKFORCE-3f, WORKFORCE-4e, WORKFORCE-4f, WORKFORCE-5c, WORKFORCE-5d, WORKFORCE-5e, WORKFORCE-5f області WORKFORCE за чотирьохбальною шкалою має бути LI або FI.

13. Визначення рівня MIL в області ARCHITECTURE:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області ARCHITECTURE рівень впровадження кожної з практик ARCHITECTURE-1a, ARCHITECTURE-2a, ARCHITECTURE-2b, ARCHITECTURE-3a, ARCHITECTURE-3b, ARCHITECTURE-5a області ARCHITECTURE за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області ARCHITECTURE рівень впровадження кожної з практик ARCHITECTURE-1a, ARCHITECTURE-2a, ARCHITECTURE-2b, ARCHITECTURE-3a, ARCHITECTURE-3b, ARCHITECTURE-5a, ARCHITECTURE-1b, ARCHITECTURE-1c, ARCHITECTURE-1d, ARCHITECTURE-1e, ARCHITECTURE-1f, ARCHITECTURE-1g, ARCHITECTURE-2c, ARCHITECTURE-2d, ARCHITECTURE-2e, ARCHITECTURE-2f, ARCHITECTURE-2g, ARCHITECTURE-3c, ARCHITECTURE-3d, ARCHITECTURE-3e, ARCHITECTURE-3f, ARCHITECTURE-3g, ARCHITECTURE-3h, ARCHITECTURE-3i, ARCHITECTURE-3j, ARCHITECTURE-3k, ARCHITECTURE-4a, ARCHITECTURE-4b, ARCHITECTURE-4c, ARCHITECTURE-5b, ARCHITECTURE-5c, ARCHITECTURE-5d, ARCHITECTURE-5e, ARCHITECTURE-5f, ARCHITECTURE-6a, ARCHITECTURE-6b області ARCHITECTURE за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області ARCHITECTURE рівень впровадження кожної з практик ARCHITECTURE-1a, ARCHITECTURE-2a, ARCHITECTURE-2b, ARCHITECTURE-3a, ARCHITECTURE-3b, ARCHITECTURE-5a, ARCHITECTURE-1b, ARCHITECTURE-1c, ARCHITECTURE-1d, ARCHITECTURE-1e, ARCHITECTURE-1f, ARCHITECTURE-1g, ARCHITECTURE-2c, ARCHITECTURE-2d, ARCHITECTURE-2e, ARCHITECTURE-2f, ARCHITECTURE-2g, ARCHITECTURE-3c, ARCHITECTURE-3d, ARCHITECTURE-3e, ARCHITECTURE-3f, ARCHITECTURE-3g, ARCHITECTURE-3h, ARCHITECTURE-3i, ARCHITECTURE-3j, ARCHITECTURE-3k, ARCHITECTURE-4a, ARCHITECTURE-4b, ARCHITECTURE-4c, ARCHITECTURE-5b, ARCHITECTURE-5c, ARCHITECTURE-5d, ARCHITECTURE-5e, ARCHITECTURE-5f, ARCHITECTURE-6a, ARCHITECTURE-6b, ARCHITECTURE-1h, ARCHITECTURE-1i, ARCHITECTURE-1j, ARCHITECTURE-1k, ARCHITECTURE-2h, ARCHITECTURE-2i, ARCHITECTURE-2j, ARCHITECTURE-2k, ARCHITECTURE-2l, ARCHITECTURE-3l, ARCHITECTURE-3m, ARCHITECTURE-4d, ARCHITECTURE-4e, ARCHITECTURE-4f, ARCHITECTURE-4g, ARCHITECTURE-4h, ARCHITECTURE-5g, ARCHITECTURE-5h, ARCHITECTURE-6c, ARCHITECTURE-6d, ARCHITECTURE-6e, ARCHITECTURE-6f області ARCHITECTURE за чотирьохбальною шкалою має бути LI або FI.

14. Визначення рівня MIL в області PROGRAM:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області PROGRAM рівень впровадження кожної з практик PROGRAM-1a,

PROGRAM-2a області PROGRAM за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області PROGRAM рівень впровадження кожної з практик PROGRAM-1a, PROGRAM-2a, PROGRAM-1b, PROGRAM-1c, PROGRAM-1d, PROGRAM-1e, PROGRAM-1f, PROGRAM-1g, PROGRAM-2b, PROGRAM-2c, PROGRAM-2d, PROGRAM-2e, PROGRAM-2f, PROGRAM-3a, PROGRAM-3b області PROGRAM за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області PROGRAM рівень впровадження кожної з практик PROGRAM-1a, PROGRAM-2a, PROGRAM-1b, PROGRAM-1c, PROGRAM-1d, PROGRAM-1e, PROGRAM-1f, PROGRAM-1g, PROGRAM-2b, PROGRAM-2c, PROGRAM-2d, PROGRAM-2e, PROGRAM-2f, PROGRAM-3a, PROGRAM-3b, PROGRAM-1h, PROGRAM-2g, PROGRAM-2h, PROGRAM-2i, PROGRAM-2j, PROGRAM-3c, PROGRAM-3d, PROGRAM-3e, PROGRAM-3f області PROGRAM за чотирьохбальною шкалою має бути LI або FI.

Додаток
до Методики оцінювання
стану кібербезпеки
електричних мереж

Індикатори та індекси
стану кібербезпеки електричних мереж

1. Модель C2M2 використовує 4 рівні MIL для визначення подвійного прогресу зрілості (прогресу підходу та прогресу управління).

2. Значення MIL мають діапазон від MIL0 до MIL3 і призначені для незалежного застосування до кожної області:

1) MIL0 – практики не виконуються;

2) MIL1 – початкові практики виконуються, але можуть бути ситуативними;

3) MIL2 – дії документуються. Дії та ініціативи забезпечені належними ресурсами і при впровадженні керуються стандартами та керівними принципами;

4) MIL3 – управління та політики кібербезпеки спрямовують дії, визначено вимоги відповідності, виконуються перевірки для забезпечення відповідності вимогам, визначені відповідальність, підзвітність та повноваження персоналу оператора, у якого також є належні навички та знання у сфері кібербезпеки.

3. Кожна з практик має один рівень MIL з наявних чотирьох (від MIL0 до MIL3).

4. Аспекти рівнів MIL, що є важливими для розуміння та застосування моделі C2M2:

1) рівні MIL застосовуються незалежно до кожної області. У результаті оператор, який використовує модель C2M2, може працювати з різними рейтингами MIL у різних областях;

2) індекси MIL (від MIL0 до MIL3) накопичуються в кожній області. Щоб отримати MIL у певній області, оператор повинен виконати всі практики на поточному рівні MIL та на попередньому рівні MIL;

3) в інструментах самооцінки моделі C2M2 практика вважається виконаною, якщо вибрано відповідь LI або FI.

5. Визначення рівня MIL в області ASSET:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області ASSET рівень впровадження кожної з практик ASSET-1a, ASSET-2a, ASSET-3a, ASSET-4a, ASSET-4b області ASSET за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області ASSET рівень впровадження кожної практик ASSET-1a, ASSET-2a, ASSET-3a, ASSET-4a, ASSET-4b, ASSET-1b, ASSET-1c, ASSET-1d, ASSET-1e, ASSET-2b, ASSET-2c, ASSET-2d, ASSET-2e, ASSET-3b, ASSET-3c, ASSET-3d, ASSET-4c, ASSET-4d, ASSET-4e, ASSET-4f, ASSET-4g, ASSET-5a, ASSET-5b області ASSET за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області ASSET рівень впровадження кожної з практик ASSET-1a, ASSET-2a, ASSET-3a, ASSET-4a, ASSET-4b, ASSET-1b, ASSET-1c, ASSET-1d, ASSET-1e, ASSET-2b, ASSET-2c, ASSET-2d, ASSET-2e, ASSET-3b, ASSET-3c, ASSET-3d, ASSET-4c, ASSET-4d, ASSET-4e, ASSET-4f, ASSET-4g, ASSET-5a, ASSET-5b, ASSET-1f, ASSET-1g, ASSET-1h, ASSET-2f, ASSET-2g, ASSET-2h, ASSET-3e, ASSET-4h, ASSET-4i, ASSET-5c, ASSET-5d, ASSET-5e, ASSET-5f області ASSET за чотирьохбальною шкалою має бути LI або FI;

6. Визначення рівня MIL в області THREAT:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області THREAT рівень впровадження кожної з практик THREAT-1a, THREAT-1b, THREAT-1c, THREAT-1d, THREAT-2a, THREAT-2b, THREAT-2c, THREAT-2d області THREAT за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області THREAT рівень впровадження кожної з практик THREAT-1a, THREAT-1b, THREAT-1c, THREAT-1d, THREAT-2a, THREAT-2b, THREAT-2c, THREAT-2d, THREAT-1e, THREAT-1f, THREAT-1g, THREAT-1h, THREAT-1i, THREAT-2e, THREAT-2f, THREAT-2g, THREAT-2h, THREAT-3a, THREAT-3b області THREAT за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області THREAT рівень впровадження кожної з практик THREAT-1a, THREAT-1b, THREAT-1c, THREAT-1d, THREAT-2a, THREAT-2b, THREAT-2c, THREAT-2d, THREAT-1e, THREAT-1f, THREAT-1g, THREAT-1h, THREAT-1i, THREAT-2e,

THREAT-2f, THREAT-2g, THREAT-2h, THREAT-3a, THREAT-3b, THREAT-1j, THREAT-1k, THREAT-1l, THREAT-1m, THREAT-2i, THREAT-2j, THREAT-2k, THREAT-3c, THREAT-3d, THREAT-3e, THREAT-3f області THREAT за чотирьохбальною шкалою має бути LI або FI.

7. Визначення рівня MIL в області RISK:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області RISK рівень впровадження кожної з практик RISK-1a, RISK-2a, RISK-3a, RISK-4a області RISK за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області RISK рівень впровадження кожної з практик RISK-1a, RISK-2a, RISK-3a, RISK-4a, RISK-1b, RISK-1c, RISK-1d, RISK-1e, RISK-1f, RISK-2b, RISK-2c, RISK-2d, RISK-2e, RISK-2f, RISK-2g, RISK-3b, RISK-3c, RISK-3d, RISK-3e, RISK-3f, RISK-4b, RISK-5a, RISK-5b області RISK за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області RISK рівень впровадження кожної з практик RISK-1a, RISK-2a, RISK-3a, RISK-4a, RISK-1b, RISK-1c, RISK-1d, RISK-1e, RISK-1f, RISK-2b, RISK-2c, RISK-2d, RISK-2e, RISK-2f, RISK-2g, RISK-3b, RISK-3c, RISK-3d, RISK-3e, RISK-3f, RISK-4b, RISK-5a, RISK-5b, RISK-1g, RISK-1h, RISK-2h, RISK-2i, RISK-2j, RISK-2k, RISK-2l, RISK-2m, RISK-3g, RISK-4c, RISK-4d, RISK-4e, RISK-5c, RISK-5d, RISK-5e, RISK-5f області RISK за чотирьохбальною шкалою має бути LI або FI;

8. Визначення рівня MIL в області ACCESS:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області ACCESS рівень впровадження кожної з практик ACCESS-1a, ACCESS-1b, ACCESS-1c, ACCESS-2a, ACCESS-2b, ACCESS-3a, ACCESS-3b, ACCESS-3c області ACCESS за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області ACCESS рівень впровадження кожної з практик ACCESS-1a, ACCESS-1b, ACCESS-1c, ACCESS-2a, ACCESS-2b, ACCESS-3a, ACCESS-3b, ACCESS-3c, ACCESS-1d, ACCESS-1e, ACCESS-1f, ACCESS-1g, ACCESS-1h, ACCESS-2c, ACCESS-2d, ACCESS-2e, ACCESS-2f, ACCESS-2g, ACCESS-3d, ACCESS-3e, ACCESS-3f, ACCESS-3g, ACCESS-3h, ACCESS-4a, ACCESS-4b області ACCESS за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області ACCESS рівень впровадження кожної з практик ACCESS-1a, ACCESS-1b,

ACCESS-1c, ACCESS-2a, ACCESS-2b, ACCESS-3a, ACCESS-3b, ACCESS-3c, ACCESS-1d, ACCESS-1e, ACCESS-1f, ACCESS-1g, ACCESS-1h, ACCESS-2c, ACCESS-2d, ACCESS-2e, ACCESS-2f, ACCESS-2g, ACCESS-3d, ACCESS-3e, ACCESS-3f, ACCESS-3g, ACCESS-3h, ACCESS-4a, ACCESS-4b, ACCESS-1i, ACCESS-1j, ACCESS-2h, ACCESS-2i, ACCESS-3i, ACCESS-3j, ACCESS-4c, ACCESS-4d, ACCESS-4e, ACCESS-4f області ACCESS за чотирьохбальною шкалою має бути LI або FI.

9. Визначення рівня MIL в області SITUATION:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області SITUATION рівень впровадження кожної з практик SITUATION-1a, SITUATION-2a, SITUATION-2b області SITUATION за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області SITUATION рівень впровадження кожної з практик SITUATION-1a, SITUATION-2a, SITUATION-2b, SITUATION-1b, SITUATION-1c, SITUATION-1d, SITUATION-1e, SITUATION-2c, SITUATION-2d, SITUATION-2e, SITUATION-2f, SITUATION-3a, SITUATION-3b, SITUATION-3c, SITUATION-4a, SITUATION-4b області SITUATION за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області SITUATION рівень впровадження кожної з практик SITUATION-1a, SITUATION-2a, SITUATION-2b, SITUATION-1b, SITUATION-1c, SITUATION-1d, SITUATION-1e, SITUATION-2c, SITUATION-2d, SITUATION-2e,SITUATION-2f, SITUATION-3a, SITUATION-3b, SITUATION-3c, SITUATION-4a, SITUATION-4b, SITUATION-1f, SITUATION-2g, SITUATION-2h, SITUATION-2i, SITUATION-3d, SITUATION-3e, SITUATION-3f, SITUATION-3g, SITUATION-4c, SITUATION-4d, SITUATION-4e, SITUATION-4f області SITUATION за чотирьохбальною шкалою має бути LI або FI.

10. Визначення рівня MIL в області RESPONSE:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області RESPONSE рівень впровадження кожної з практик RESPONSE-1a, RESPONSE-2a, RESPONSE-2b, RESPONSE-3a, RESPONSE-3b, RESPONSE-3c, RESPONSE-4a, RESPONSE-4b, RESPONSE-4c області RESPONSE за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області RESPONSE рівень впровадження кожної з практик RESPONSE-1a,

RESPONSE-2a, RESPONSE-2b, RESPONSE-3a, RESPONSE-3b, RESPONSE-3c, RESPONSE-4a, RESPONSE-4b, RESPONSE-4c, RESPONSE-1b, RESPONSE-1c, RESPONSE-2c, RESPONSE-2d, RESPONSE-2e, RESPONSE-2f, RESPONSE-2g, RESPONSE-3d, RESPONSE-3e, RESPONSE-3f, RESPONSE-3g, RESPONSE-3h, RESPONSE-4d, RESPONSE-4e, RESPONSE-4f, RESPONSE-4g, RESPONSE-4h, RESPONSE-4i, RESPONSE-4j, RESPONSE-4k, RESPONSE-4l, RESPONSE-5a, RESPONSE-5b області RESPONSE за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області RESPONSE рівень впровадження кожної з практик RESPONSE-1a, RESPONSE-2a, RESPONSE-2b, RESPONSE-3a, RESPONSE-3b, RESPONSE-3c, RESPONSE-4a, RESPONSE-4b, RESPONSE-4c, RESPONSE-1b, RESPONSE-1c, RESPONSE-2c, RESPONSE-2d, RESPONSE-2e, RESPONSE-2f, RESPONSE-2g, RESPONSE-3d, RESPONSE-3e, RESPONSE-3f, RESPONSE-3g, RESPONSE-3h, RESPONSE-4d, RESPONSE-4e, RESPONSE-4f, RESPONSE-4g, RESPONSE-4h, RESPONSE-4i, RESPONSE-4j, RESPONSE-4k, RESPONSE-4l, RESPONSE-5a, RESPONSE-5b, RESPONSE-1d RESPONSE-1e RESPONSE-1f RESPONSE-2h RESPONSE-2i RESPONSE-3i RESPONSE-3j RESPONSE-3k RESPONSE-3l RESPONSE-4m RESPONSE-4n RESPONSE-4o RESPONSE-4p RESPONSE-5c RESPONSE-5d RESPONSE-5e RESPONSE-5f області RESPONSE за чотирьохбальною шкалою має бути LI або FI.

11. Визначення рівня MIL в області THIRD-PARTIES:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області THIRD-PARTIES рівень впровадження кожної з практик THIRD-PARTIES-1a, THIRD-PARTIES-1b, THIRD-PARTIES-2a, THIRD-PARTIES-2b області THIRD-PARTIES за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області THIRD-PARTIES рівень впровадження кожної з практик THIRD-PARTIES-1a, THIRD-PARTIES-1b, THIRD-PARTIES-2a, THIRD-PARTIES-2b, THIRD-PARTIES-1c, THIRD-PARTIES-1d, THIRD-PARTIES-1e, THIRD-PARTIES-2c, THIRD-PARTIES-2d, THIRD-PARTIES-2e, THIRD-PARTIES-2f, THIRD-PARTIES-2g, THIRD-PARTIES-3a, THIRD-PARTIES-3b області THIRD-PARTIES за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області THIRD-PARTIES рівень впровадження кожної з практик THIRD-PARTIES-1a, THIRD-PARTIES-1b, THIRD-PARTIES-2a, THIRD-PARTIES-2b, THIRD-PARTIES-1c THIRD-PARTIES-1d, THIRD-PARTIES-1e, THIRD-PARTIES-2c, THIRD-PARTIES-2d, THIRD-PARTIES-2e,

THIRD-PARTIES-2f, THIRD-PARTIES-2g, THIRD-PARTIES-3a, THIRD-PARTIES-3b, THIRD-PARTIES-1f, THIRD-PARTIES-2h, THIRD-PARTIES-2i, THIRD-PARTIES-2j, THIRD-PARTIES-2k, THIRD-PARTIES-2l, THIRD-PARTIES-2m, THIRD-PARTIES-3c, THIRD-PARTIES-3d, THIRD-PARTIES-3e, THIRD-PARTIES-3f області THIRD-PARTIES за чотирьохбальною шкалою має бути LI або FI.

12. Визначення рівня MIL в області WORKFORCE:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області WORKFORCE рівень впровадження кожної з практик WORKFORCE-1a, WORKFORCE-1b, WORKFORCE-2a, WORKFORCE-3a, WORKFORCE-3b, WORKFORCE-4a, WORKFORCE-4b області WORKFORCE за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області WORKFORCE рівень впровадження кожної з практик WORKFORCE-1a, WORKFORCE-1b, WORKFORCE-2a, WORKFORCE-3a, WORKFORCE-3b, WORKFORCE-4a, WORKFORCE-4b, WORKFORCE-1c, WORKFORCE-1d, WORKFORCE-1e, WORKFORCE-2b, WORKFORCE-2c, WORKFORCE-2d, WORKFORCE-3c, WORKFORCE-3d, WORKFORCE-4c, WORKFORCE-4d, WORKFORCE-5a, WORKFORCE-5b області WORKFORCE за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області WORKFORCE рівень впровадження кожної з практик WORKFORCE-1a, WORKFORCE-1b, WORKFORCE-2a, WORKFORCE-3a, WORKFORCE-3b, WORKFORCE-4a, WORKFORCE-4b, WORKFORCE-1c, WORKFORCE-1d, WORKFORCE-1e, WORKFORCE-2b, WORKFORCE-2c, WORKFORCE-2d, WORKFORCE-3c, WORKFORCE-3d, WORKFORCE-4c, WORKFORCE-4d, WORKFORCE-5a, WORKFORCE-5b, WORKFORCE-1f WORKFORCE-1g WORKFORCE-2e WORKFORCE-2f, WORKFORCE-2g, WORKFORCE-3e, WORKFORCE-3f, WORKFORCE-4e, WORKFORCE-4f, WORKFORCE-5c, WORKFORCE-5d, WORKFORCE-5e, WORKFORCE-5f області WORKFORCE за чотирьохбальною шкалою має бути LI або FI.

13. Визначення рівня MIL в області ARCHITECTURE:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області ARCHITECTURE рівень впровадження кожної з практик ARCHITECTURE-1a, ARCHITECTURE-2a, ARCHITECTURE-2b, ARCHITECTURE-3a, ARCHITECTURE-3b, ARCHITECTURE-5a області ARCHITECTURE за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області ARCHITECTURE рівень впровадження кожної з практик ARCHITECTURE-1a, ARCHITECTURE-2a, ARCHITECTURE-2b, ARCHITECTURE-3a, ARCHITECTURE-3b, ARCHITECTURE-5a, ARCHITECTURE-1b, ARCHITECTURE-1c, ARCHITECTURE-1d, ARCHITECTURE-1e, ARCHITECTURE-1f, ARCHITECTURE-1g, ARCHITECTURE-2c, ARCHITECTURE-2d, ARCHITECTURE-2e, ARCHITECTURE-2f, ARCHITECTURE-2g, ARCHITECTURE-3c, ARCHITECTURE-3d, ARCHITECTURE-3e, ARCHITECTURE-3f, ARCHITECTURE-3g, ARCHITECTURE-3h, ARCHITECTURE-3i, ARCHITECTURE-3j, ARCHITECTURE-3k, ARCHITECTURE-4a, ARCHITECTURE-4b, ARCHITECTURE-4c, ARCHITECTURE-5b, ARCHITECTURE-5c, ARCHITECTURE-5d, ARCHITECTURE-5e, ARCHITECTURE-5f, ARCHITECTURE-6a, ARCHITECTURE-6b області ARCHITECTURE за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області ARCHITECTURE рівень впровадження кожної з практик ARCHITECTURE-1a, ARCHITECTURE-2a, ARCHITECTURE-2b, ARCHITECTURE-3a, ARCHITECTURE-3b, ARCHITECTURE-5a, ARCHITECTURE-1b, ARCHITECTURE-1c, ARCHITECTURE-1d, ARCHITECTURE-1e, ARCHITECTURE-1f, ARCHITECTURE-1g, ARCHITECTURE-2c, ARCHITECTURE-2d, ARCHITECTURE-2e, ARCHITECTURE-2f, ARCHITECTURE-2g, ARCHITECTURE-3c, ARCHITECTURE-3d, ARCHITECTURE-3e, ARCHITECTURE-3f, ARCHITECTURE-3g, ARCHITECTURE-3h, ARCHITECTURE-3i, ARCHITECTURE-3j, ARCHITECTURE-3k, ARCHITECTURE-4a, ARCHITECTURE-4b, ARCHITECTURE-4c, ARCHITECTURE-5b, ARCHITECTURE-5c, ARCHITECTURE-5d, ARCHITECTURE-5e, ARCHITECTURE-5f, ARCHITECTURE-6a, ARCHITECTURE-6b, ARCHITECTURE-1h, ARCHITECTURE-1i, ARCHITECTURE-1j, ARCHITECTURE-1k, ARCHITECTURE-2h, ARCHITECTURE-2i, ARCHITECTURE-2j, ARCHITECTURE-2k, ARCHITECTURE-2l, ARCHITECTURE-3l, ARCHITECTURE-3m, ARCHITECTURE-4d, ARCHITECTURE-4e, ARCHITECTURE-4f, ARCHITECTURE-4g, ARCHITECTURE-4h, ARCHITECTURE-5g, ARCHITECTURE-5h, ARCHITECTURE-6c, ARCHITECTURE-6d, ARCHITECTURE-6e, ARCHITECTURE-6f області ARCHITECTURE за чотирьохбальною шкалою має бути LI або FI.

14. Визначення рівня MIL в області PROGRAM:

1) для досягнення індикатора зрілості MIL1 моделі C2M2 в області PROGRAM рівень впровадження кожної з практик PROGRAM-1a,

PROGRAM-2a області PROGRAM за чотирьохбальною шкалою має бути LI або FI;

2) для досягнення індикатора зрілості MIL2 моделі C2M2 в області PROGRAM рівень впровадження кожної з практик PROGRAM-1a, PROGRAM-2a, PROGRAM-1b, PROGRAM-1c, PROGRAM-1d, PROGRAM-1e, PROGRAM-1f, PROGRAM-1g, PROGRAM-2b, PROGRAM-2c, PROGRAM-2d, PROGRAM-2e, PROGRAM-2f, PROGRAM-3a, PROGRAM-3b області PROGRAM за чотирьохбальною шкалою має бути LI або FI;

3) для досягнення індикатора зрілості MIL3 моделі C2M2 в області PROGRAM рівень впровадження кожної з практик PROGRAM-1a, PROGRAM-2a, PROGRAM-1b, PROGRAM-1c, PROGRAM-1d, PROGRAM-1e, PROGRAM-1f, PROGRAM-1g, PROGRAM-2b, PROGRAM-2c, PROGRAM-2d, PROGRAM-2e, PROGRAM-2f, PROGRAM-3a, PROGRAM-3b, PROGRAM-1h, PROGRAM-2g, PROGRAM-2h, PROGRAM-2i, PROGRAM-2j, PROGRAM-3c, PROGRAM-3d, PROGRAM-3e, PROGRAM-3f області PROGRAM за чотирьохбальною шкалою має бути LI або FI.

ЗАТВЕРДЖЕНО

Наказ Міністерства енергетики України
_____ № _____

Зміни
до Плану діяльності Міністерства енергетики України
з підготовки проектів регуляторних актів на 2024 рік

Доповнити план позиціями такого змісту:

№ з/п	Назва проекту регуляторного акта	Обґрунтування необхідності прийняття регуляторного акта	Центральні органи виконавчої влади, структурні підрозділи, що розроблятимуть регуляторний акт	Термін виконання
34.	Постанова Кабінету Міністрів України «Деякі питання проведення експертизи технічних умов приєднання (вихідних даних) до газотранспортної або газорозподільної системи на відповідність чинним стандартам, нормам та правилам»	Врегулювання процедури проведення незалежної експертизи технічних умов приєднання (вихідних даних) до газотранспортної або газорозподільної системи	Директорат нафтогазового комплексу та розвитку ринків нафти, природного газу та нафтопродуктів	III квартал 2024 року
35.	Наказ Міністерства енергетики України «Про затвердження Правил доступу суб'єктів ринку природного газу	Врегулювання відносин між замовником та виконавцем Послуги переміщення природного газу	Директорат нафтогазового комплексу та	III квартал 2024 року

	до газопроводів, що становлять частину інфраструктури родовища нафти і газу або призначені для переміщення видобутого природного газу від місцезнаходження родовища до станції переробки»	внутрішньопромисловими газопроводами; визначення правових, технічних, організаційних та економічних засад доступу суб'єктів ринку природного газу до газопроводів, що становлять частину інфраструктури родовища нафти і газу або призначені для переміщення видобутого природного газу від місцезнаходження родовища до станції переробки, з метою надання послуги переміщення природного газу такими газопроводами	розвитку ринків нафти, природного газу та нафтопродуктів	
36.	Наказ Міністерства енергетики України «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж»	Визначення моделі зрілості спроможностей кібербезпеки електричних мереж, як об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури	Управління захисту критичної інфраструктури, кібербезпеки та цифрового розвитку	III квартал 2024 року

_____

МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ
(Міненерго)
вул. Хрещатик, 30, м. Київ, 01601, тел.: (044) 531-36-93; 206-38-45
E-mail: kanc@mev.gov.ua, сайт: https://www.mev.gov.ua, ідентифікаційний код 37552996

_____ На № _____

Державна регуляторна служба України

Щодо погодження проєкту наказу

Міністерство енергетики України надсилає на розгляд проєкт наказу Міненерго «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж» (далі – проєкт наказу), розроблений відповідно до пункту 2 Плану заходів щодо реалізації Концепції впровадження «розумних мереж» в Україні до 2035 року, затвердженого розпорядженням Кабінету Міністрів України від 14.10.2022 № 908-р, з урахуванням доручення Прем'єр-міністра України Дениса ШМИГАЛЯ від 28.03.2024 № 40517/8/1-23, та просить погодити проєкт наказу **в триденний термін**.

Додатки: 1. Проєкт наказу на 51 арк.
2. Аналіз регуляторного впливу до проєкту наказу на 11 арк.
3. Повідомлення про оприлюднення проєкту наказу на 2 арк.
4. Копія наказу від 29 травня 2024 року № 203 «Про внесення змін до Плану діяльності Міністерства енергетики України з підготовки проектів регуляторних актів на 2024 рік» на 3 арк.

Міністр **Герман ГАЛУЩЕНКО**

Ірина ГОНЧАРЕНКО +380686741786

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики України
«__»_____2024 року №_____

Методика
оцінювання стану кібербезпеки електричних мереж

1. Ця Методика визначає модель зрілості спроможностей кібербезпеки електричних мереж (далі – модель зрілості), як об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури та/або їх систем, їх частин та їх сукупностей (далі – електричні мережі).

2. Дія цієї Методики поширюється на операторів критичної інфраструктури (далі – оператори), що на правах власності, оренди або на інших законних підставах здійснюють управління електричними мережами.

3. У цій Методиці терміни вживаються у таких значеннях:

1) модель C2M2 – модель зрілості спроможностей кібербезпеки електричних мереж для оцінки та вдосконалення програм з кібербезпеки електричних мереж та зміцнення їх експлуатаційної стійкості;

2) зрілість – вимірювана здатність оператора постійно вдосконалюватися в межах кібербезпеки електричних мереж;

3) показник зрілості кібербезпеки електричних мереж – параметр стану кібербезпеки електричних мереж;

4) оцінка стану кібербезпеки електричних мереж – визначення або вимірювання показників зрілості кібербезпеки електричних мереж;

5) індекс кібербезпеки електричних мереж (далі – індекс MIL) – періодичні інформаційні матеріали, які містять експертні, аналітичні, статистичні відомості про стан кібербезпеки електричних мереж, а також про окремі показники шкідливого впливу реалізованих кіберзагроз, складені з метою оцінки стану кібербезпеки електричних мереж;

6) індикатор зрілості кібербезпеки (далі – індикатор зрілості) – значення показника зрілості кібербезпеки електричних мереж;

7) модель зрілості – структурований набір практик, інструкцій, планів дій для створення ефективних програм з кібербезпеки електричних мереж та проведення заходів з кіберзахисту електричних мереж;

8) рівень кібербезпеки електричних мереж (далі – рівень MIL) – рівень індикатора зрілості моделі C2M2, який визначається сукупністю практик кібербезпеки електричних мереж (далі – практика) з області кібербезпеки електричних мереж (далі – область), що впроваджені та виконуються в електричних мережах;

9) практика – це метод, пов'язаний з діями, які багаторазово виконуються в межах кібербезпеки електричних мереж, що і визначають міру рівня зрілості спроможностей кібербезпеки електричних мереж;

10) область – це логічне групування практик.

Кожен такий набір практик представляє діяльність, яку оператори виконують для встановлення та розвитку спроможностей у сфері кібербезпеки електричних мереж;

11) активи інформаційних технологій (далі – IT-активи) – окремий набір електронних інформаційних ресурсів, організованих для збору, обробки, підтримки, використання, спільного використання, розповсюдження або розміщення інформації.

Це визначення включає взаємопов'язані або взаємозалежні системи та середовище, в якому вони працюють.

До IT-активів належать робочі станції, комутатори, маршрутизатори, міжмережеві екрани, сервери, віртуальні машини, програмне забезпечення, мобільні комп'ютерні пристрої, хмарні активи;

12) активи операційних технологій (далі – OT-активи) – активи, які знаходяться у сегменті операційних технологій електричних мереж та необхідні для надання послуг або виробничої діяльності.

Більшість систем керування електричними мережами включають IT-активи.

До OT-активів належать робочі станції, комутатори, маршрутизатори, міжмережеві екрани, сервери, віртуальні машини, програмне забезпечення, мобільні комп'ютерні пристрої, хмарні активи, програмовані логічні контролери, віддалені термінали, промислові системи управління (ICS), системи безпеки, пристрої контролю фізичного доступу;

13) інформаційні активи – будь-яке повідомлення або представлення знань, таких як факти, дані, які є цінними для електричних мереж.

Інформаційні активи можуть бути в будь-якому носії чи формі, включаючи цифрові чи нецифрові. До інформаційних активів належать бізнес-дані, інтелектуальна власність, інформація про клієнтів, контракти, договори,

журнали безпеки, метадані, оперативні дані, фінансові дані, інформація про безпеку та журнали керування подіями, файли конфігурації.

Інші терміни вживаються у значеннях, наведених у Законах України «Про критичну інфраструктуру», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про ринок електричної енергії».

4. Метою цієї Методики є визначення алгоритму оцінки та вдосконалення програм з кібербезпеки електричних мереж.

5. Модель C2M2:

1) формулює модель зрілості як сукупність характеристик, атрибутів, показників або зразків, що показують спроможності та прогрес реалізації заходів з кіберзахисту електричних мереж;

2) визначає управління практикою реалізації кібербезпеки електричних мереж та адаптована для використання операторами;

3) призначена для використання операторами з метою здійснення самооцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж.

Для ефективної реалізації моделі C2M2 найкраще використовувати її як частину безперервного процесу управління ризиками електричних мереж.

6. Формою застосування моделі C2M2 є самооцінка оператором електричних мереж, що здійснюється по мірі необхідності, але не рідше 1 разу на рік.

7. За результатами застосування моделі C2M2 оператор готує звіт, що надсилається Міненерго протягом 10 днів, але не пізніше 01 грудня поточного року.

У звіті зазначаються:

дані про поточний стан кібербезпеки електричних мереж;

дані про реалізацію оператором заходів з кіберзахисту електричних мереж за результатами застосування моделі C2M2;

дані про вдосконалення програм оператора з кібербезпеки електричних мереж за результатами застосування моделі C2M2.

8. У моделі C2M2 термін «функція» відноситься до електричних мереж.

9. Модель C2M2 широко визначає поняття «функція», щоб надати операторам найбільший ступінь гнучкості у визначенні обсягу самооцінки, яка підходить для них.

10. Вибір функції визначає, які об'єкти критичної інформаційної інфраструктури (далі – об'єкти), інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, автоматизовані системи управління технологічними процесами електричних мереж підлягатимуть оцінці, включаючи взаємопов'язані або взаємозалежні системи та середовище, в якому вони працюють.

11. Для цілей моделі C2M2 термін «активи» включає всі об'єкти, інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, автоматизовані системи управління технологічними процесами електричних мереж в рамках вибраної функції, включаючи взаємопов'язані або взаємозалежні системи та середовище, в якому вони працюють.

12. Модель C2M2 включає 356 практик, які класифіковані в 10 областей.

13. Кожна область асоціюється з унікальною ціллю управління та кількома цілями підходу. У рамках цілей як підходу, так і цілей управління деталізовані практики для опису діяльності з кібербезпеки електричних мереж. У межах кожної цілі практики впорядковані за рівнями MIL.

14. Для вимірювання прогресу моделі C2M2 використовують шкалу, що визначає рівні від MIL0 до MIL3 згідно з додатком до цієї Методики. Набір практик визначає кожен рівень MIL. Якщо оператор впровадив та використовує такий набір практик, то він досяг як цього рівня MIL, так і можливостей, які цей рівень MIL представляє.

15. Наявність вимірних перехідних станів між рівнями MIL дозволяє використовувати шкалу для:

1) визначення поточного стану електричних мереж щодо кібербезпеки;

2) визначення майбутнього, більш зрілого стану кібербезпеки електричних мереж;

3) визначення можливостей, які оператор повинен забезпечити, щоб досягти майбутнього показника зрілості стану кібербезпеки електричних мереж.

16. Області моделі C2M2:

1) ASSET – управління активами, змінами та конфігурацією. Управління IT-активами та OT-активами електричних мереж, включаючи апаратне та програмне забезпечення, а також інформаційні активи відповідно до ризику кібербезпеки для електричних мереж;

2) THREAT – управління загрозами та вразливістю. Створення та підтримка планів, процедур та технологій для виявлення, ідентифікації, аналізу, керування та реагування на загрози та вразливості кібербезпеки електричних мереж відповідно до ризику кібербезпеки для них;

3) RISK – управління ризиками. Управління IT-активами та OT-активами електричних мереж, включаючи апаратне та програмне забезпечення, а також інформаційні активи відповідно до ризику кібербезпеки для електричних мереж;

4) ACCESS – управління ідентифікацією та доступом. Створення ідентифікаційних даних для активів, яким може бути надано логічний або фізичний доступ до активів електричних мереж, керування ними. Контроль доступу до активів електричних мереж відповідно до ризику кібербезпеки для них;

5) SITUATION – ситуаційна обізнаність. Впровадження та підтримка заходів і технологій для збору, моніторингу, аналізу, попередження, звітування та використання операційної інформації, інформації про безпеку та загрози, включаючи інформацію про статус і зведену інформацію з інших областей моделі C2M2, щоб отримати ситуаційну обізнаність щодо робочого стану кібербезпеки електричних мереж;

6) RESPONSE – реагування на події та інциденти. Створення та підтримка планів, процедур та технологій для виявлення, аналізу, реагування на події та інциденти кібербезпеки електричних мереж та відновлення після них, а також підтримка роботи під час інцидентів кібербезпеки електричних мереж відповідно до ризику кібербезпеки для них;

7) THIRD-PARTIES – управління ланцюгами постачання та зовнішніми взаємозалежностями. Встановлення та підтримка засобів контролю для управління кіберризиками, що виникають при взаємодії з постачальниками послуг електричних мереж, відповідно до ризику кібербезпеки для електричних мереж та цілей оператора;

8) WORKFORCE – управління персоналом. Створення та підтримка планів, процедур, технологій і засобів контролю кібербезпеки електричних мереж та забезпечення сталої компетентності персоналу з кібербезпеки відповідно до ризику кібербезпеки для електричних мереж та цілей оператора;

9) ARCHITECTURE – архітектура кібербезпеки. Створення та підтримка архітектури кібербезпеки електричних мереж, включаючи засоби контролю, процеси, технології та інші елементи;

10) PROGRAM – управління програмою кібербезпеки електричних мереж. Створення і підтримка програми кібербезпеки електричних мереж, яка забезпечує управління, стратегічне планування та фінансову підтримку діяльності електричних мереж з кібербезпеки таким чином, щоб цілі з кібербезпеки були узгоджені із стратегічними цілями та ризиками для об'єкту критичної інфраструктури в цілому.

17. Модель C2M2 призначена для використання методології самооцінки оператором з метою вимірювання та вдосконалення власної програми з кібербезпеки електричних мереж.

18. Застосування моделі C2M2 здійснюється шляхом вибору рівня провадження кожної практики з використанням чотирибальної шкали:

не виконано (NI) – практика не проводиться;

частково виконано (PI) – виконання не завершено, є багато можливостей для вдосконалення;

переважно виконано (LI) – здебільшого виконано, але є можливість вдосконалення;

повністю виконано (FI) – реалізовано у повній мірі.

19. Визначення рівня MIL для кожної області є ефективною стратегією використання моделі C2M2 для вдосконалення програми кібербезпеки електричних мереж. Операторам необхідно ознайомитися з практиками в моделі C2M2 до визначення рівнів MIL.

20. Практична ефективність і досягнення рівнів MIL повинні узгоджуватися зі стратегією програми кібербезпеки електричних мереж. Прагнення досягти найвищого рівня MIL у всіх областях може бути не оптимальним. Необхідно оцінити витрати на досягнення конкретного рівня MIL порівняно з його потенційними перевагами.

Заступник начальника
Управління – начальник відділу
цифрової трансформації Управління
захисту критичної інфраструктури,
кібербезпеки та цифрового розвитку **Віталій БАЗАЛИЦЬКИЙ**

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики України
«__»_____2024 року №_____

Методика
оцінювання стану кібербезпеки електричних мереж

1. Ця Методика визначає модель зрілості спроможностей кібербезпеки електричних мереж (далі – модель зрілості), як об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури та/або їх систем, їх частин та їх сукупностей (далі – електричні мережі).

2. Дія цієї Методики поширюється на операторів критичної інфраструктури (далі – оператори), що на правах власності, оренди або на інших законних підставах здійснюють управління електричними мережами.

3. У цій Методиці терміни вживаються у таких значеннях:

1) модель C2M2 – модель зрілості спроможностей кібербезпеки електричних мереж для оцінки та вдосконалення програм з кібербезпеки електричних мереж та зміцнення їх експлуатаційної стійкості;

2) зрілість – вимірювана здатність оператора постійно вдосконалюватися в межах кібербезпеки електричних мереж;

3) показник зрілості кібербезпеки електричних мереж – параметр стану кібербезпеки електричних мереж;

4) оцінка стану кібербезпеки електричних мереж – визначення або вимірювання показників зрілості кібербезпеки електричних мереж;

5) індекс кібербезпеки електричних мереж (далі – індекс MIL) – періодичні інформаційні матеріали, які містять експертні, аналітичні, статистичні відомості про стан кібербезпеки електричних мереж, а також про окремі показники шкідливого впливу реалізованих кіберзагроз, складені з метою оцінки стану кібербезпеки електричних мереж;

6) індикатор зрілості кібербезпеки (далі – індикатор зрілості) – значення показника зрілості кібербезпеки електричних мереж;

7) модель зрілості – структурований набір практик, інструкцій, планів дій для створення ефективних програм з кібербезпеки електричних мереж та проведення заходів з кіберзахисту електричних мереж;

8) рівень кібербезпеки електричних мереж (далі – рівень MIL) – рівень індикатора зрілості моделі C2M2, який визначається сукупністю практик кібербезпеки електричних мереж (далі – практика) з області кібербезпеки електричних мереж (далі – область), що впроваджені та виконуються в електричних мережах;

9) практика – це метод, пов'язаний з діями, які багаторазово виконуються в межах кібербезпеки електричних мереж, що і визначають міру рівня зрілості спроможностей кібербезпеки електричних мереж;

10) область – це логічне групування практик.

Кожен такий набір практик представляє діяльність, яку оператори виконують для встановлення та розвитку спроможностей у сфері кібербезпеки електричних мереж;

11) активи інформаційних технологій (далі – IT-активи) – окремий набір електронних інформаційних ресурсів, організованих для збору, обробки, підтримки, використання, спільного використання, розповсюдження або розміщення інформації.

Це визначення включає взаємопов'язані або взаємозалежні системи та середовище, в якому вони працюють.

До IT-активів належать робочі станції, комутатори, маршрутизатори, міжмережеві екрани, сервери, віртуальні машини, програмне забезпечення, мобільні комп'ютерні пристрої, хмарні активи;

12) активи операційних технологій (далі – OT-активи) – активи, які знаходяться у сегменті операційних технологій електричних мереж та необхідні для надання послуг або виробничої діяльності.

Більшість систем керування електричними мережами включають IT-активи.

До OT-активів належать робочі станції, комутатори, маршрутизатори, міжмережеві екрани, сервери, віртуальні машини, програмне забезпечення, мобільні комп'ютерні пристрої, хмарні активи, програмовані логічні контролери, віддалені термінали, промислові системи управління (ICS), системи безпеки, пристрої контролю фізичного доступу;

13) інформаційні активи – будь-яке повідомлення або представлення знань, таких як факти, дані, які є цінними для електричних мереж.

Інформаційні активи можуть бути в будь-якому носії чи формі, включаючи цифрові чи нецифрові. До інформаційних активів належать бізнес-дані, інтелектуальна власність, інформація про клієнтів, контракти, договори,

журнали безпеки, метадані, оперативні дані, фінансові дані, інформація про безпеку та журнали керування подіями, файли конфігурації.

Інші терміни вживаються у значеннях, наведених у Законах України «Про критичну інфраструктуру», «Про основні засади забезпечення кібербезпеки України», «Про захист інформації в інформаційно-комунікаційних системах», «Про ринок електричної енергії».

4. Метою цієї Методики є визначення алгоритму оцінки та вдосконалення програм з кібербезпеки електричних мереж.

5. Модель C2M2:

1) формулює модель зрілості як сукупність характеристик, атрибутів, показників або зразків, що показують спроможності та прогрес реалізації заходів з кіберзахисту електричних мереж;

2) визначає управління практикою реалізації кібербезпеки електричних мереж та адаптована для використання операторами;

3) призначена для використання операторами з метою здійснення самооцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж.

Для ефективної реалізації моделі C2M2 найкраще використовувати її як частину безперервного процесу управління ризиками електричних мереж.

6. Формою застосування моделі C2M2 є самооцінка оператором електричних мереж, що здійснюється по мірі необхідності, але не рідше 1 разу на рік.

7. За результатами застосування моделі C2M2 оператор готує звіт, що надсилається Міненерго протягом 10 днів, але не пізніше 01 грудня поточного року.

У звіті зазначаються:

дані про поточний стан кібербезпеки електричних мереж;

дані про реалізацію оператором заходів з кіберзахисту електричних мереж за результатами застосування моделі C2M2;

дані про вдосконалення програм оператора з кібербезпеки електричних мереж за результатами застосування моделі C2M2.

8. У моделі C2M2 термін «функція» відноситься до електричних мереж.

9. Модель C2M2 широко визначає поняття «функція», щоб надати операторам найбільший ступінь гнучкості у визначенні обсягу самооцінки, яка підходить для них.

10. Вибір функції визначає, які об'єкти критичної інформаційної інфраструктури (далі – об'єкти), інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, автоматизовані системи управління технологічними процесами електричних мереж підлягатимуть оцінці, включаючи взаємопов'язані або взаємозалежні системи та середовище, в якому вони працюють.

11. Для цілей моделі C2M2 термін «активи» включає всі об'єкти, інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, автоматизовані системи управління технологічними процесами електричних мереж в рамках вибраної функції, включаючи взаємопов'язані або взаємозалежні системи та середовище, в якому вони працюють.

12. Модель C2M2 включає 356 практик, які класифіковані в 10 областей.

13. Кожна область асоціюється з унікальною ціллю управління та кількома цілями підходу. У рамках цілей як підходу, так і цілей управління деталізовані практики для опису діяльності з кібербезпеки електричних мереж. У межах кожної цілі практики впорядковані за рівнями MIL.

14. Для вимірювання прогресу моделі C2M2 використовують шкалу, що визначає рівні від MIL0 до MIL3 згідно з додатком до цієї Методики. Набір практик визначає кожен рівень MIL. Якщо оператор впровадив та використовує такий набір практик, то він досяг як цього рівня MIL, так і можливостей, які цей рівень MIL представляє.

15. Наявність вимірних перехідних станів між рівнями MIL дозволяє використовувати шкалу для:

1) визначення поточного стану електричних мереж щодо кібербезпеки;

2) визначення майбутнього, більш зрілого стану кібербезпеки електричних мереж;

3) визначення можливостей, які оператор повинен забезпечити, щоб досягти майбутнього показника зрілості стану кібербезпеки електричних мереж.

16. Області моделі C2M2:

1) ASSET – управління активами, змінами та конфігурацією. Управління IT-активами та OT-активами електричних мереж, включаючи апаратне та програмне забезпечення, а також інформаційні активи відповідно до ризику кібербезпеки для електричних мереж;

2) THREAT – управління загрозами та вразливістю. Створення та підтримка планів, процедур та технологій для виявлення, ідентифікації, аналізу, керування та реагування на загрози та вразливості кібербезпеки електричних мереж відповідно до ризику кібербезпеки для них;

3) RISK – управління ризиками. Управління IT-активами та OT-активами електричних мереж, включаючи апаратне та програмне забезпечення, а також інформаційні активи відповідно до ризику кібербезпеки для електричних мереж;

4) ACCESS – управління ідентифікацією та доступом. Створення ідентифікаційних даних для активів, яким може бути надано логічний або фізичний доступ до активів електричних мереж, керування ними. Контроль доступу до активів електричних мереж відповідно до ризику кібербезпеки для них;

5) SITUATION – ситуаційна обізнаність. Впровадження та підтримка заходів і технологій для збору, моніторингу, аналізу, попередження, звітування та використання операційної інформації, інформації про безпеку та загрози, включаючи інформацію про статус і зведену інформацію з інших областей моделі C2M2, щоб отримати ситуаційну обізнаність щодо робочого стану кібербезпеки електричних мереж;

6) RESPONSE – реагування на події та інциденти. Створення та підтримка планів, процедур та технологій для виявлення, аналізу, реагування на події та інциденти кібербезпеки електричних мереж та відновлення після них, а також підтримка роботи під час інцидентів кібербезпеки електричних мереж відповідно до ризику кібербезпеки для них;

7) THIRD-PARTIES – управління ланцюгами постачання та зовнішніми взаємозалежностями. Встановлення та підтримка засобів контролю для управління кіберризиками, що виникають при взаємодії з постачальниками послуг електричних мереж, відповідно до ризику кібербезпеки для електричних мереж та цілей оператора;

8) WORKFORCE – управління персоналом. Створення та підтримка планів, процедур, технологій і засобів контролю кібербезпеки електричних мереж та забезпечення сталої компетентності персоналу з кібербезпеки відповідно до ризику кібербезпеки для електричних мереж та цілей оператора;

9) ARCHITECTURE – архітектура кібербезпеки. Створення та підтримка архітектури кібербезпеки електричних мереж, включаючи засоби контролю, процеси, технології та інші елементи;

10) PROGRAM – управління програмою кібербезпеки електричних мереж. Створення і підтримка програми кібербезпеки електричних мереж, яка забезпечує управління, стратегічне планування та фінансову підтримку діяльності електричних мереж з кібербезпеки таким чином, щоб цілі з кібербезпеки були узгоджені із стратегічними цілями та ризиками для об'єкту критичної інфраструктури в цілому.

17. Модель C2M2 призначена для використання методології самооцінки оператором з метою вимірювання та вдосконалення власної програми з кібербезпеки електричних мереж.

18. Застосування моделі C2M2 здійснюється шляхом вибору рівня провадження кожної практики з використанням чотирибальної шкали:

не виконано (NI) – практика не проводиться;

частково виконано (PI) – виконання не завершено, є багато можливостей для вдосконалення;

переважно виконано (LI) – здебільшого виконано, але є можливість вдосконалення;

повністю виконано (FI) – реалізовано у повній мірі.

19. Визначення рівня MIL для кожної області є ефективною стратегією використання моделі C2M2 для вдосконалення програми кібербезпеки електричних мереж. Операторам необхідно ознайомитися з практиками в моделі C2M2 до визначення рівнів MIL.

20. Практична ефективність і досягнення рівнів MIL повинні узгоджуватися зі стратегією програми кібербезпеки електричних мереж. Прагнення досягти найвищого рівня MIL у всіх областях може бути не оптимальним. Необхідно оцінити витрати на досягнення конкретного рівня MIL порівняно з його потенційними перевагами.

Заступник начальника
Управління – начальник відділу
цифрової трансформації Управління
захисту критичної інфраструктури,
кібербезпеки та цифрового розвитку **Віталій БАЗАЛИЦЬКИЙ**

МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

_____ **м. Київ** **_____**

Про внесення змін до Плану діяльності Міністерства енергетики України з підготовки проектів регуляторних актів на 2024 рік

Відповідно до Закону України «Про засади державної регуляторної політики у сфері господарської діяльності»; постанови Кабінету Міністрів України від 17 червня 2020 року № 507 «Про затвердження Положення про Міністерство енергетики України»; Положення про державну реєстрацію нормативно-правових актів міністерств, інших органів виконавчої влади, затвердженого постановою Кабінету Міністрів України від 28 грудня 1992 року № 731,

НАКАЗУЮ:

1. Затвердити зміни до Плану діяльності Міністерства енергетики України з підготовки проектів регуляторних актів на 2024 рік, затвердженого наказом Міністерства енергетики України від 08 грудня 2023 року № 377 (зі змінами), що додаються.

2. Контроль за виконанням цього наказу залишаю за собою.

Міністр **Герман ГАЛУЩЕНКО**

МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

_____ **м. Київ** _____

Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж

Відповідно до пункту 2 Плану заходів щодо реалізації Концепції впровадження «розумних мереж» в Україні до 2035 року, затвердженого розпорядженням Кабінету Міністрів України від 14 жовтня 2022 року № 908-р, пункту 8 Положення про Міністерство енергетики України, затвердженого постановою Кабінету Міністрів України від 17 червня 2020 року № 507,
НАКАЗУЮ:

1. Затвердити такі, що додаються:

1) Методику оцінювання стану кібербезпеки електричних мереж;

2) Практики кібербезпеки електричних мереж.

2. Управлінню захисту критичної інфраструктури, кібербезпеки та цифрового розвитку забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому порядку.

3. Цей наказ набирає чинності з дня його офіційного опублікування.

4. Контроль за виконанням цього наказу покласти на заступника Міністра відповідно до розподілу функціональних обов'язків.

Міністр **Герман ГАЛУЩЕНКО**

МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ

Н А К А З

_____ **м. Київ** _____

Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж

Відповідно до пункту 2 Плану заходів щодо реалізації Концепції впровадження «розумних мереж» в Україні до 2035 року, затвердженого розпорядженням Кабінету Міністрів України від 14 жовтня 2022 року № 908-р, пункту 8 Положення про Міністерство енергетики України, затвердженого постановою Кабінету Міністрів України від 17 червня 2020 року № 507,
НАКАЗУЮ:

1. Затвердити такі, що додаються:

1) Методику оцінювання стану кібербезпеки електричних мереж;

2) Практики кібербезпеки електричних мереж.

2. Управлінню захисту критичної інфраструктури, кібербезпеки та цифрового розвитку забезпечити подання цього наказу на державну реєстрацію до Міністерства юстиції України в установленому порядку.

3. Цей наказ набирає чинності з дня його офіційного опублікування.

4. Контроль за виконанням цього наказу покласти на заступника Міністра відповідно до розподілу функціональних обов'язків.

Міністр **Герман ГАЛУЩЕНКО**

Міністерство енергетики України

Міністерство енергетики України

Повідомлення про оприлюднення проєкту наказу Міністерства енергетики України «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж»

Повідомлення про оприлюднення проєкту наказу Міністерства енергетики України «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж»

Проєкт акта розроблений Міністерством енергетики України з метою визначення моделі зрілості спроможностей кібербезпеки електричних мереж, як об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури.

Зауваження та пропозиції слід надсилати на адреси: Міністерство енергетики України, 01601, м. Київ, вул. Б. Хмельницького, 4; e-mail: iryna.honcharenko@mev.gov.ua

Державна регуляторна служба України, 01011 м. Київ, вул. Арсенальна, 9/11;
e- mail: inform@dkrp.gov.ua

Проєкт регуляторного акта та аналіз регуляторного впливу оприлюднені шляхом розміщення на офіційному веб-сайті Міненерго в мережі інтернет https://www.mev.gov.ua/. Зауваження та пропозиції від фізичних та юридичних осіб, їх об'єднань приймаються протягом місяця з дати оприлюднення в письмовому або електронному вигляді.

Документи:

1. Проєкт Наказу;
2. Пояснювальна записка;
3. Аналіз регуляторного впливу;
4. Практики;
5. Методика;
6. Додаток до Методики.

Проєкт Наказу	151.79 КБ
Пояснювальна записка	398.07 КБ
Аналіз регуляторного впливу	498.48 КБ

UB
Міністерство енергетики України
№20-1.1-10.2-12862 від 31.05.2024
КЕП: Галущенко Г. В. 31.05.2024 10:20
3ED5083160DBC59B040000007CDD0600BFB5FF00
Сертифікат дійсний з 01.05.2023 17:01 по 01.05.2025 17:01

Методика	2.49 МБ
Додаток до Методики	235.23 КБ

Дата публікації 27 травня 2024, 14:15

Категорія Повідомлення про оприлюднення

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики України
«__»_____2024 року № _____

Практики
кібербезпеки електричних мереж

№ з/п	Ідентифікатор практики	MIL	Опис практики	Рівень впровадження			
				NI	PI	LI	FI
1	2	3	4	5	6	7	8
Область: Управління активами, змінами та конфігурацією (ASSET)							
Ціль 1. Управління інвентаризацією IT-активів та OT-активів							
1	ASSET -1a	1	IT-активи та OT-активи, важливі для виконання функції, інвентаризуються, принаймні в певному порядку.				
2	ASSET -1b	2	Інвентаризація IT-активів та OT-активів включає активи в межах функції, які можуть бути використані для досягнення мети загрози.				
3	ASSET -1c	2	Інвентаризовані IT-активи та OT-активи встановлюються за пріоритетністю на основі визначених критеріїв, які включають важливість для виконання функції.				
4	ASSET -1d	2	Критерії визначення пріоритетів включають розгляд ступеня, до якого актив у межах функції може бути використаний для досягнення цілі загрози.				
5	ASSET -1e	2	Інвентаризація IT-активів та OT-активів містить атрибути, які підтримують дії з кібербезпеки (наприклад, розташування, пріоритет активів, власник активів, операційна система та версії прошивки).				

1	2	3	4	5	6	7	8
6	ASSET -1f	3	Інвентаризацію IT-активів та OT-активів завершено (інвентаризація включає всі активи в межах функції).				
7	ASSET -1g	3	Інвентаризація IT-активів та OT-активів є актуальною, тобто періодично оновлюється відповідно до визначених тригерів, наприклад системних змін.				
8	ASSET -1h	3	Дані знищуються або безпечно видаляються з IT-активів та OT-активів перед перерозподілом і в кінці терміну служби.				
Ціль 2. Управління інвентаризацією інформаційних активів							
9	ASSET -2a	1	Інформаційні активи, які є важливими для виконання функції (наприклад, задані значення SCADA та інформація про клієнтів), інвентаризуються, принаймні в певному порядку.				
10	ASSET -2b	2	Інвентаризація інформаційних активів включає інформаційні активи в межах функції, які можуть бути використані для досягнення мети загрози.				
11	ASSET -2c	2	Інвентаризовані інформаційні активи класифікуються на основі визначених критеріїв, які враховують важливість для виконання функції.				
12	ASSET -2d	2	Критерії класифікації враховують розгляд ступеня, до якого інформаційний актив у межах функції може бути використаний для досягнення мети загрози.				
13	ASSET -2e	2	Інвентаризація інформаційних активів включає атрибути, які підтримують дії з кібербезпеки (наприклад, категорія активів, місця та частоту резервного копіювання, місця зберігання, власник активу, вимоги до кібербезпеки).				
14	ASSET -2f	2	Інвентаризація інформаційних активів завершена (інвентаризація включає всі активи в межах функції).				
15	ASSET -2g	2	Інвентаризація інформаційних активів є актуальною, тобто вона оновлюється періодично відповідно до визначених тригерів, таких як системні зміни.				

1	2	3	4	5	6	7	8
16	ASSET -2h	2	Інформаційні активи підлягають санітарній обробці або знищенню наприкінці терміну служби за допомогою методів, які відповідають вимогам кібербезпеки.				
Ціль 3. Управління конфігураціями IT-активів та OT-активів							
17	ASSET -3a	1	Базові параметри конфігурації встановлюються, принаймні, у певний спосіб.				
18	ASSET -3b	2	Базові параметри конфігурації використовуються для налаштування активів під час розгортання та відновлення.				
19	ASSET -3c	2	Базові параметри конфігурації включають відповідні вимоги архітектури кібербезпеки (практика ARCHITECTURE-1f).				
20	ASSET -3d	2	Базові параметри конфігурації періодично переглядаються та оновлюються відповідно до визначених тригерів, таких як системні зміни та зміни в архітектурі кібербезпеки.				
21	ASSET -3e	3	Конфігурації активів перевіряються на узгодженість із базовими протягом усього життєвого циклу активів.				
Ціль 4. Управління змінами в IT-активах та OT-активах							
22	ASSET -4a	1	Зміни в активах оцінюються та затверджуються перед впровадженням, принаймні в окремих випадках.				
23	ASSET -4b	1	Зміни в активах документуються, принаймні в окремих випадках.				
24	ASSET -4c	2	Вимоги до документації щодо змін у активах встановлено та підтримуються.				
25	ASSET -4d	2	Зміни до ресурсів з вищим пріоритетом тестуються перед розгортанням.				
26	ASSET -4e	2	Зміни та оновлення впроваджуються безпечним способом.				
27	ASSET -4f	2	Можливість скасовувати зміни встановлюється та підтримується для активів, які важливі для виконання функції.				

1	2	3	4	5	6	7	8
28	ASSET -4g	2	Практики управління змінами стосуються повного життєвого циклу активів (наприклад, придбання, розгортання, експлуатації та виведення з експлуатації).				
29	ASSET -4h	3	Перед розгортанням зміни в активах з вищим пріоритетом перевіряються на вплив на кібербезпеку.				
30	ASSET -4i	3	Журнали змін містять інформацію про зміни, які впливають на вимоги кібербезпеки активів.				
Ціль 5. Управління областю ASSET							
31	ASSET -5a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області ASSET.				
32	ASSET -5b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області ASSET.				
33	ASSET -5c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області ASSET.				
34	ASSET -5d	3	Відповідальність, підзвітність та повноваження щодо виконання діяльності в області ASSET покладаються на персонал.				
35	ASSET -5e	3	Персонал, який виконує діяльність у області ASSET, має навички та знання, необхідні для виконання покладених на них обов'язків				
36	ASSET -5f	3	Ефективність діяльності в області ASSET оцінюється та відстежується.				
Область: Управління загрозами та вразливостями (THREAT)							
Ціль 1. Зменшення вразливостей кібербезпеки							
37	THREAT-1a	1	Визначаються джерела інформації для підтримки виявлення вразливості кібербезпеки, принаймні в окремих випадках.				
38	THREAT-1b	1	Інформація про вразливість кібербезпеки збирається та інтерпретується для функції, принаймні в окремих випадках.				

1	2	3	4	5	6	7	8
39	THREAT-1c	1	Оцінка вразливості кібербезпеки виконується, принаймні, в разовому порядку.				
40	THREAT-1d	1	Вразливості кібербезпеки, які мають відношення до виконання функції, пом'якшуються, принаймні в окремих випадках.				
41	THREAT-1e	2	Відстежуються джерела інформації про вразливості кібербезпеки, які стосуються активів вищого пріоритету.				
42	THREAT-1f	2	Оцінка вразливості кібербезпеки виконується періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
43	THREAT-1g	2	Виявлені вразливості кібербезпеки аналізуються та встановлюються за пріоритетністю, а також усуваються відповідним чином.				
44	THREAT-1h	2	Операційний вплив на функцію оцінюється перед розгортанням виправлень або інших заходів щодо усунення вразливостей.				
45	THREAT-1i	2	Інформація про виявлені вразливості кібербезпеки передається зацікавленим сторонам, визначеним організацією.				
46	THREAT-1j	3	Відстежуються джерела інформації про вразливості кібербезпеки, які спільно стосуються всіх IT- активів та OT-активів у межах функції.				
47	THREAT-1k	3	Оцінка вразливості кібербезпеки виконується сторонами, які не залежать від операцій цієї функції.				
48	THREAT-1l	3	Діяльність з моніторингу вразливостей включає перевірку, яка підтверджує, що дії, вжиті у відповідь на вразливості кібербезпеки, були ефективними.				
49	THREAT-1m	3	Встановлюються та підтримуються механізми для отримання та реагування на звіти від громадськості чи зовнішніх сторін про потенційну вразливість, пов'язану з IT-активами та OT-активами організації, такими як загальнодоступні веб-сайти або мобільні додатки.				

1	2	3	4	5	6	7	8
Ціль 2. Реагування на загрози та обмін інформацією про загрози							
50	THREAT-2a	1	Внутрішні та зовнішні джерела інформації для підтримки діяльності з управління загрозами визначаються, принаймні в окремих випадках.				
51	THREAT-2b	1	Інформація про загрози кібербезпеці збирається та інтерпретується, принаймні в окремих випадках.				
52	THREAT-2c	1	Цілі щодо загроз для функції визначаються, принаймні, у певний спосіб.				
53	THREAT-2d	1	Загрози, які мають відношення до виконання функції, розглядаються, принаймні, у певний спосіб.				
54	THREAT-2e	2	Встановлюється профіль загрози для функції, який включає цілі загрози та додаткові характеристики загрози (наприклад, типи суб'єктів загрози, мотиви, можливості та цілі).				
55	THREAT-2f	2	Джерела інформації про загрози, які спільно стосуються всіх компонентів профілю загроз, визначаються за пріоритетністю та контролюються.				
56	THREAT-2g	2	Виявлені загрози аналізуються та встановлюються за пріоритетністю, а потім розглядаються відповідно.				
57	THREAT-2h	2	Обмін інформацією про загрози здійснюється із зацікавленими сторонами (наприклад, керівниками, оперативним персоналом, урядом, пов'язаними організаціями, постачальниками, галузевими організаціями, регуляторами, центрами обміну інформацією та аналізу).				
58	THREAT-2i	3	Профіль загроз для функції оновлюється періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
59	THREAT-2j	3	Моніторинг загроз і заходи реагування на них використовують і запускають попередньо визначені стани роботи (практика SITUATION-3g).				

1	2	3	4	5	6	7	8
60	THREAT-2k	3	Захищені методи майже в реальному часі використовуються для отримання та обміну інформацією про загрози, щоб забезпечити швидкий аналіз і дії.				
Ціль 3. Управління областю THREAT							
61	THREAT-3a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області THREAT.				
62	THREAT-3b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області THREAT.				
63	THREAT-3c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області THREAT.				
64	THREAT-3d	3	Відповідальність, підзвітність та повноваження щодо виконання діяльності в області THREAT покладаються на персонал.				
65	THREAT-3e	3	Персонал, який виконує діяльність у області THREAT, має навички та знання, необхідні для виконання покладених на нього обов'язків.				
66	THREAT-3f	3	Оцінюється та відстежується ефективність діяльності в області THREAT.				
Область: Управління ризиками (RISK)							
Ціль 1. Створення та підтримка стратегії та програми управління кіберризиками							
67	RISK-1a	1	Організація має стратегію управління кіберризиками, яка може бути розроблена та керована в індивідуальному порядку.				
68	RISK-1b	2	Стратегія управління кіберризиками створюється та підтримується відповідно до стратегії програми кібербезпеки організації (практика PROGRAM-1b) та архітектури підприємства.				
69	RISK-1c	2	Програма управління кіберризиками створена та підтримується для виконання заходів з управління кіберризиками відповідно до стратегії управління кіберризиками.				

1	2	3	4	5	6	7	8
70	RISK-1d	2	Інформація про діяльність у області RISK передається відповідним зацікавленим сторонам.				
71	RISK-1e	2	Встановлено та підтримується керування програмою управління кіберризиками.				
72	RISK-1f	2	Фінансова підтримка вищого керівництва програми управління кіберризиками є помітною та активною.				
73	RISK-1g	3	Програма управління кіберризиками відповідає місії та цілям організації.				
74	RISK-1h	3	Програма управління кіберризиками узгоджується з загальнокорпоративною програмою управління ризиками організації.				
			Ціль 2. Визначення кіберризиків				
75	RISK-2a	1	Кібернетичні ризики визначаються, принаймні час від часу.				
76	RISK-2b	2	Визначено метод, що використовується для визначення кіберризиків.				
77	RISK-2c	2	Зацікавлені сторони з відповідних операцій і бізнес-сфер беруть участь у виявленні кіберризиків.				
78	RISK-2d	2	Виявлені кіберризики консолідуються за категоріями (наприклад, порушення даних, внутрішні помилки, програми-вимагачі, захоплення контролю), щоб полегшити керування на рівні категорії.				
79	RISK-2e	2	Категорії кіберризиків і кіберризики документуються в реєстрі ризиків або в іншій формі.				
80	RISK-2f	2	Категорії кіберризиків і кіберризики призначаються власникам ризиків.				
81	RISK-2g	2	Діяльність з ідентифікації кіберризиків виконується періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				

1	2	3	4	5	6	7	8
82	RISK-2h	3	Діяльність з ідентифікації кіберризиків використовує інвентаризацію активів та інформацію про пріоритетність із області ASSET, таку як завершення підтримки IT-активів та OT-активів, одиничні точки збою, ризик розкриття, підробки або знищення інформаційних активів.				
83	RISK-2i	3	Інформація про керування вразливістю з області THREAT використовується для оновлення кіберризиків і виявлення нових ризиків (таких як ризики, що виникають через вразливості, які становлять постійний ризик для організації, або нещодавно виявлені вразливості).				
84	RISK-2j	3	Інформація про керування загрозами у області THREAT використовується для оновлення кіберризиків і виявлення нових ризиків.				
85	RISK-2k	3	Інформація про діяльність області THIRD-PARTIES використовується для оновлення кіберризиків і виявлення нових ризиків.				
86	RISK-2l	3	Інформація про дії у області ARCHITECTURE (наприклад, невиправлені прогалини в архітектурі) використовується для оновлення кіберризиків і виявлення нових ризиків.				
87	RISK-2m	3	Ідентифікація кіберризиків враховує ризики, які можуть виникнути або вплинути на інші взаємозалежні організації.				
			Ціль 3. Аналіз кіберризиків				
88	RISK-3a	1	Пріоритезація кіберризиків визначається на основі оцінки їх впливу, принаймні в окремих випадках.				
89	RISK-3b	2	Визначені критерії використовуються для визначення пріоритетності кіберризиків (наприклад, вплив на організацію, вплив на спільноту, ймовірність, сприйнятливість, толерантність до ризику).				

1	2	3	4	5	6	7	8
90	RISK-3c	2	Визначений метод використовується для оцінки впливу кіберризиків з вищим пріоритетом (наприклад, порівняння з реальними подіями, кількісна оцінка ризику).				
91	RISK-3d	2	Визначені методи використовуються для аналізу кіберризиків з вищим пріоритетом (наприклад, аналіз поширеності типів атак для оцінки ймовірності, використання результатів оцінки засобів контролю для оцінки сприйнятливості).				
92	RISK-3e	2	Організаційно зацікавлені сторони з відповідних операцій і бізнес-функцій беруть участь в аналізі кіберризиків з вищим пріоритетом.				
93	RISK-3f	2	Кіберризики видаляються з реєстру ризиків або інших форм їх фіксації, що використовуються для документування виявлених ризиків і керування ними, коли вони більше не потребують відстеження чи реагування.				
94	RISK-3g	3	Аналіз кіберризиків періодично оновлюється відповідно до визначених тригерів, таких як системні зміни, зовнішні події та інформація з інших областей моделі.				
			Ціль 4. Реагування на кіберризики				
95	RISK-4a	1	Реагування на ризики (такі як пом'якшення, прийняття, уникнення або передача) впроваджується для усунення кіберризиків, принаймні в окремих випадках.				
96	RISK-4b	2	Визначений метод використовується для вибору та впровадження заходів реагування на ризики на основі аналізу та встановлення пріоритетів.				
97	RISK-4c	3	Засоби контролю кібербезпеки оцінюються, щоб визначити, чи вони розроблені належним чином і чи функціонують за їх призначенням -для зменшення виявлених кіберризиків.				
98	RISK-4d	3	Результати аналізу впливу кіберризиків і оцінки контролю кібербезпеки разом переглядаються керівництвом				

1	2	3	4	5	6	7	8
			підприємства, щоб визначити, чи достатньо пом'якшено кіберризики та чи не перевищено допустимі рівні ризику.				
99	RISK-4e	3	Реакції на ризики (такі як пом'якшення, прийняття, уникнення або передача) періодично переглядаються керівництвом, щоб визначити, чи вони все ще доцільні.				
Ціль 5. Управління в області RISK							
100	RISK-5a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області RISK.				
101	RISK-5b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області RISK.				
102	RISK-5c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області RISK.				
103	RISK-5d	3	Відповідальність, підзвітність та повноваження щодо виконання діяльності в області RISK покладаються на персонал.				
104	RISK-5e	3	Персонал, який виконує діяльність у області RISK, має навички та знання, необхідні для виконання покладених на них обов'язків.				
105	RISK-5f	3	Оцінюється та відстежується ефективність діяльності в області RISK.				
Область: Управління ідентифікацією та доступом (ACCESS)							
Ціль 1. Встановлення ідентичності та керування автентифікацією							
106	ACCESS-1a	1	Ідентифікаційні дані надаються, принаймні в певному порядку, для персоналу та інших об'єктів, таких як служби та пристрої, яким потрібен доступ до активів (зверніть увагу, що це не виключає спільних ідентифікаційних даних).				
107	ACCESS-1b	1	Облікові дані (такі як паролі, смарт-карти, сертифікати та ключі) видаються персоналу та іншим особам, яким потрібен доступ до активів, принаймні в тимчасовому порядку.				

1	2	3	4	5	6	7	8
108	ACCESS-1c	1	Ідентифікаційні дані деініціалізуються, принаймні тимчасово, коли вони більше не потрібні.				
109	ACCESS-1d	2	Обмеження щодо надійності пароля та повторного його використання визначені та застосовуються.				
110	ACCESS-1e	2	Репозиторії ідентифікаційних даних переглядаються та оновлюються періодично та відповідно до визначених тригерів, таких як системні зміни та зміни організаційної структури.				
111	ACCESS-1f	2	Ідентифікаційні дані деініціалізуються в межах часу, визначеного організацією, коли вони більше не потрібні.				
112	ACCESS-1g	2	Використання привілейованих облікових даних обмежено процесами, для яких вони потрібні.				
113	ACCESS-1h	2	Для доступу з підвищеним ризиком (наприклад, привілейовані облікові записи, облікові записи служб, спільні облікові записи та віддалений доступ) використовуються надійніші облікові дані, багатофакторна автентифікація або одноразові облікові дані.				
114	ACCESS-1i	3	Багатофакторна автентифікація потрібна для будь-якого доступу, де це можливо.				
115	ACCESS-1j	3	Ідентифікаційні дані вимикаються після певного періоду бездіяльності, де це можливо.				
			Ціль 2. Контроль логічного доступу				
116	ACCESS-2a	1	Реалізовано логічний контроль доступу, принаймні, у певний спосіб.				
117	ACCESS-2b	1	Привілеї логічного доступу скасовуються, коли більше не потрібні, принаймні інколи.				
118	ACCESS-2c	2	Встановлюються та підтримуються вимоги до логічного доступу (наприклад, правила, яким типам об’єктів дозволено доступ до активу, обмеження дозволеного доступу, обмеження віддаленого доступу, параметри автентифікації).				

1	2	3	4	5	6	7	8
119	ACCESS-2d	2	Вимоги до логічного доступу включають принцип найменших привілеїв.				
120	ACCESS-2e	2	Вимоги до логічного доступу включають принцип розподілу обов'язків.				
121	ACCESS-2f	2	Запити на логічний доступ переглядаються та затверджуються власником ресурсу.				
122	ACCESS-2g	2	Привілеї логічного доступу, які становлять більший ризик для функції, отримують додаткову перевірку та моніторинг.				
123	ACCESS-2h	3	Логічні привілеї доступу переглядаються та оновлюються для забезпечення відповідності вимогам доступу періодично та відповідно до визначених тригерів, таких як зміни в організаційній структурі, і після будь-якого тимчасового підвищення привілеїв.				
124	ACCESS-2i	3	Аномальні спроби отримати логічний доступ відстежуються як індикатори подій кібербезпеки.				
			Ціль 3. Контроль фізичного доступу				
125	ACCESS-3a	1	Фізичні засоби контролю доступу (такі як огорожі, замки та вивіски) реалізовані, принаймні в певному порядку.				
126	ACCESS-3b	1	Привілеї фізичного доступу скасовуються, коли вони більше не потрібні, принаймні інколи.				
127	ACCESS-3c	1	Журнали фізичного доступу зберігаються, принаймні в певному порядку.				
128	ACCESS-3d	2	Вимоги до фізичного доступу встановлюються та підтримуються (наприклад, правила щодо того, хто має доступ до активу, як надається доступ, обмеження дозволеного доступу).				
129	ACCESS-3e	2	Вимоги щодо фізичного доступу включають принцип найменших привілеїв.				

1	2	3	4	5	6	7	8
130	ACCESS-3f	2	Вимоги щодо фізичного доступу включають принцип розподілу обов'язків.				
131	ACCESS-3g	2	Запити на фізичний доступ розглядаються та затверджуються власником ресурсу.				
132	ACCESS-3h	2	Привілеї фізичного доступу, які створюють підвищений ризик для функції, отримують додаткову перевірку та моніторинг.				
133	ACCESS-3i	3	Привілеї фізичного доступу переглядаються та оновлюються.				
134	ACCESS-3j	3	Фізичний доступ відстежується для виявлення потенційних подій кібербезпеки.				
Ціль 4. Управління в області ACCESS							
135	ACCESS-4a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області ACCESS.				
136	ACCESS-4b	2	Для підтримки діяльності в області ACCESS надаються відповідні ресурси (люди, фінансування та інструменти).				
137	ACCESS-4c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області ACCESS.				
138	ACCESS-4d	3	Відповідальність, підзвітність та повноваження щодо виконання діяльності в області ACCESS покладаються на персонал.				
139	ACCESS-4e	3	Персонал, який виконує діяльність у області ACCESS, має навички та знання, необхідні для виконання покладених на них обов'язків.				
140	ACCESS-4f	3	Ефективність діяльності в області ACCESS оцінюється та відстежується.				
Область: Ситуаційна обізнаність (SITUATION)							
Ціль 1. Виконання журналювання							
141	SITUATION -1a	1	Реєстрація ведеться для активів, які важливі для виконання функції, принаймні одноразово.				

1	2	3	4	5	6	7	8
142	SITUATION-1b	2	Журналювання проводиться де це можливо для активів у операціях, які можуть бути використані для досягнення мети загрози.				
143	SITUATION-1c	2	Вимоги до журналювання встановлюються та підтримуються для IT-активів та OT-активів, важливих для виконання функції, і активів у межах функції, які можуть бути використані для досягнення цілі загрози.				
144	SITUATION-1d	2	Вимоги до журналювання встановлюються та підтримуються для інфраструктури моніторингу мережі та хостів (наприклад, веб-шлюзи, програмне забезпечення для виявлення і реагування на кінцевих точках, системи виявлення та запобігання вторгненням).				
145	SITUATION-1e	2	Дані журналу агрегуються у межах функції.				
146	SITUATION-1f	3	Ретельніше журналювання виконується для активів з вищим пріоритетом.				
			Ціль 2. Проведення моніторингу				
147	SITUATION-2a	1	Виконуються періодичні перевірки даних журналів або інші заходи моніторингу кібербезпеки, принаймні в разовому порядку.				
148	SITUATION-2b	1	Дані та сповіщення з мережевих і хост-моніторингових активів інфраструктури періодично переглядаються, принаймні в разовому порядку.				
149	SITUATION-2c	2	Вимоги до моніторингу та аналізу встановлюються та підтримуються для функції та забезпечують своєчасний перегляд даних про події.				
150	SITUATION-2d	2	Індикатори аномальної активності встановлюються та підтримуються на основі системних журналів, потоків даних, базових показників мережі, подій кібербезпеки та архітектури				

1	2	3	4	5	6	7	8
			та відстежуються в середовищах як інформаційних так операційних технологій.				
151	SITUATION-2e	2	Сигнали тривоги та сповіщення налаштовані та підтримуються для підтримки ідентифікації подій кібербезпеки.				
152	SITUATION-2f	2	Діяльність моніторингу узгоджується з профілем загроз (практика THREAT-2e).				
153	SITUATION-2g	3	Ретельніший моніторинг здійснюється для активів з вищим пріоритетом.				
154	SITUATION-2h	3	Інформація аналізу ризиків (практика RISK-3d) використовується для визначення показників аномальної активності.				
155	SITUATION-2i	3	Індикатори аномальної активності оцінюються та оновлюються періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
Ціль 3. Створення та підтримка обізнаності про ситуацію							
156	SITUATION-3a	2	Методи передачі інформації про поточний стан кібербезпеки для функції встановлено та підтримуються.				
157	SITUATION-3b	2	Дані моніторингу агрегируються, щоб забезпечити розуміння робочого стану функції.				
158	SITUATION-3c	2	Відповідна інформація з усієї організації доступна для підвищення обізнаності про ситуацію.				
159	SITUATION-3d	3	Було визначено вимоги до звітності щодо обізнаності про ситуацію, які стосуються своєчасного розповсюдження інформації про кібербезпеку зацікавленим сторонам, визначеним організацією.				
160	SITUATION-3e	3	Релевантна інформація ззовні організації збирається та стає доступною в усій організації для підвищення обізнаності про ситуацію.				

1	2	3	4	5	6	7	8
161	SITUATION-3f	3	Встановлено та підтримується можливість агрегирувати, співвідносити та аналізувати результати діяльності моніторингу кібербезпеки та надавати майже в реальному часі розуміння стану кібербезпеки функції.				
162	SITUATION-3g	3	Попередньо визначені стани роботи задокументовані та можуть бути реалізовані на основі стану кібербезпеки функції або коли вони викликані діяльністю в інших областях.				
Ціль 4. Управління у області SITUATION							
163	SITUATION-4a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області SITUATION.				
164	SITUATION-4b	2	Достатні ресурси (люди, фінансування та інструменти) надаються для підтримки діяльності в області SITUATION.				
165	SITUATION-4c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області SITUATION.				
166	SITUATION-4d	3	Відповідальність, підзвітність та повноваження щодо виконання заходів у області SITUATION покладаються на персонал.				
167	SITUATION-4e	3	Персонал, який виконує діяльність у області SITUATION, має навички та знання, необхідні для виконання покладених на нього обов'язків.				
168	SITUATION-4f	3	Оцінюється та відстежується ефективність діяльності в області SITUATION.				
Область: Реагування на події та інциденти, безперервність роботи (RESPONSE)							
Ціль 1. Виявлення події кібербезпеки							
169	RESPONSE-1a	1	Виявлені події кібербезпеки повідомляються певній особі або ролі та документуються, принаймні в певному порядку.				
170	RESPONSE-1b	2	Встановлюються критерії для виявлення подій кібербезпеки (наприклад, що є подією кібербезпеки, де шукати події кібербезпеки).				

1	2	3	4	5	6	7	8
171	RESPONSE-1c	2	Події кібербезпеки документуються на основі встановлених критеріїв.				
172	RESPONSE-1d	3	Інформація про події корелюється для підтримки аналізу інцидентів шляхом виявлення закономірностей, тенденцій та інших загальних характеристик.				
173	RESPONSE-1e	3	Діяльність виявлення подій кібербезпеки коригується на основі виявлених ризиків і профілю загрози організації (практика THREAT-2e).				
174	RESPONSE-1f	3	Ситуаційна обізнаність для функції контролюється для підтримки ідентифікації подій кібербезпеки.				
Ціль 2. Аналіз подій кібербезпеки та оголошення про інциденти							
175	RESPONSE-2a	1	Критерії для оголошення інцидентів кібербезпеки встановлюються, принаймні в окремих випадках.				
176	RESPONSE-2b	1	Події кібербезпеки аналізуються, щоб підтвердити декларування про інциденти кібербезпеки, принаймні в окремих випадках.				
177	RESPONSE-2c	2	Критерії декларування інцидентів кібербезпеки формально встановлюються на основі потенційного впливу на функцію.				
178	RESPONSE-2d	2	Події кібербезпеки оголошуються інцидентами на основі встановлених критеріїв.				
179	RESPONSE-2e	2	Критерії декларування інцидентів кібербезпеки періодично оновлюються відповідно до визначених тригерів, таких як організаційні зміни, висновки, отримані під час виконання плану з кіберзахисту, або нещодавно виявлені загрози.				
180	RESPONSE-2f	2	Є репозиторій, де події та інциденти кібербезпеки документуються та відстежуються до закриття.				
181	RESPONSE-2g	2	Внутрішні та зовнішні зацікавлені сторони (наприклад, керівники, юристи, державні установи, пов'язані організації, постачальники, галузеві організації, регулятори) визначаються				

1	2	3	4	5	6	7	8
			та повідомляються про інциденти на основі вимог щодо звітності про ситуацію (практика SITUATION-3d).				
182	RESPONSE-2h	3	Критерії для декларування інцидентів кібербезпеки узгоджені з критеріями пріоритетності кіберризиків (практика RISK-3b).				
183	RESPONSE-2i	3	Інциденти кібербезпеки порівнюються, аналізуються, щоб визначити закономірності, тенденції та інші загальні характеристики в кількох інцидентах.				
Ціль 3. Реагування на інциденти кібербезпеки							
184	RESPONSE-3a	1	Визначається персонал задіяний у реагуванні на інциденти кібербезпеки та розподіляються ролі, принаймні в окремих випадках.				
185	RESPONSE-3b	1	Реагування на інциденти кібербезпеки виконується, принаймні, у певний спосіб, щоб обмежити вплив на функцію та відновити нормальну роботу.				
186	RESPONSE-3c	1	Звітування про інциденти здійснюється (наприклад, внутрішня звітність, CERT-UA, тощо), принаймні в разовому порядку.				
187	RESPONSE-3d	2	Розробляються та підтримуються плани реагування на інциденти кібербезпеки, які стосуються всіх етапів життєвого циклу інциденту.				
188	RESPONSE-3e	2	Реагування на інциденти кібербезпеки виконується відповідно до визначених планів і процедур.				
189	RESPONSE-3f	2	Плани реагування на інциденти кібербезпеки включають план комунікацій для внутрішніх і зовнішніх зацікавлених сторін.				
190	RESPONSE-3g	2	Навчання плану реагування на інциденти кібербезпеки проводяться періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
191	RESPONSE-3h	2	Виконуються заходи на основі отриманих уроків щодо інцидентів кібербезпеки та вживаються коригувальні дії, включаючи оновлення плану реагування на інциденти.				

1	2	3	4	5	6	7	8
192	RESPONSE-3i	3	Виконується аналіз основних причин інциденту кібербезпеки та вживаються коригувальні дії, включаючи оновлення плану реагування на інциденти.				
193	RESPONSE-3j	3	Реагування на інциденти кібербезпеки узгоджується з постачальниками, правоохоронними органами та іншими зовнішніми організаціями, якщо це необхідно, включаючи підтримку збору та збереження доказів.				
194	RESPONSE-3k	3	Персонал з реагування на інциденти кібербезпеки бере участь у спільних навчаннях з кібербезпеки з іншими організаціями.				
195	RESPONSE-3l	3	Реагування на інциденти кібербезпеки використовує та запускає попередньо визначені режими роботи (практика SITUATION-3g).				
Ціль 4. Вирішення проблеми кібербезпеки в безперервності операцій							
196	RESPONSE-4a	1	Розробляються плани безперервності, щоб підтримувати та відновлювати роботу функції, якщо трапляється подія чи інцидент у сфері кібербезпеки, принаймні випадково.				
197	RESPONSE-4b	1	Резервне копіювання даних доступне та протестоване, принаймні в разовому порядку.				
198	RESPONSE-4c	1	IT-активи та OT-активи, які потребують запасних частин, визначаються, принаймні, в окремих випадках.				
199	RESPONSE-4d	2	У планах забезпечення безперервності розглядаються потенційні наслідки інцидентів кібербезпеки.				
200	RESPONSE-4e	2	Активи та діяльність, необхідні для підтримки мінімальних операцій функції, визначаються та документуються в планах безперервності.				
201	RESPONSE-4f	2	Плани забезпечення безперервності стосуються IT-активів, OT-активів та інформаційних активів, які важливі для виконання функцій, включаючи наявність резервних копій даних і їх заміни, надлишкових та резервних IT-активів і OT-активів.				

1	2	3	4	5	6	7	8
202	RESPONSE-4g	2	Цільові показники часу відновлення (RTO) і точки відновлення (RPO) для активів, які важливі для виконання функції, включені до планів безперервності.				
203	RESPONSE-4h	2	Критерії інциденту кібербезпеки, які ініціюють виконання планів безперервності, встановлюються та повідомляються персоналу з реагування на інциденти та управління безперервністю.				
204	RESPONSE-4i	2	Плани безперервності перевіряються за допомогою оцінювання та періодичних вправ відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
205	RESPONSE-4j	2	Контроль кібербезпеки, що захищає резервні дані, еквівалентний або більш суворий, ніж контроль, що захищає вихідні дані.				
206	RESPONSE-4k	2	Резервні копії даних логічно або фізично відокремлені від вихідних даних.				
207	RESPONSE-4l	2	Доступні запчастини для вибраних IT- та OT-активів.				
208	RESPONSE-4m	3	Плани безперервності узгоджені з виявленими ризиками та профілем загроз організації (практика THREAT-2e), щоб забезпечити покриття визначених категорій ризиків і загроз.				
209	RESPONSE-4n	3	Навчання плану безперервності стосуються ризиків вищого пріоритету.				
210	RESPONSE-4o	3	Результати тестування або активації плану безперервності порівнюються з цілями відновлення, і плани відповідно вдосконалюються.				
211	RESPONSE-4p	3	Плани безперервності періодично переглядаються та оновлюються.				
Ціль 5. Управління областю RESPONSE							
212	RESPONSE-5a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області RESPONSE.				

1	2	3	4	5	6	7	8
213	RESPONSE-5b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області RESPONSE.				
214	RESPONSE-5c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області RESPONSE.				
215	RESPONSE-5d	3	Відповідальність, підзвітність та повноваження щодо здійснення діяльності у області RESPONSE покладено на персонал.				
216	RESPONSE-5e	3	Персонал, який виконує діяльність у області RESPONSE, має навички та знання, необхідні для виконання покладених на них обов'язків.				
217	RESPONSE-5f	3	Оцінюється та відстежується ефективність діяльності в області RESPONSE.				
Область: Управління ланцюгами постачання та зовнішніми взаємозалежностями (THIRD-PARTIES)							
Ціль 1. Виявлення третіх сторін і визначення пріоритетів							
218	THIRD-PARTIES-1a	1	Визначаються важливі залежності інформаційних та операційних технологій від третіх сторін (тобто внутрішні та зовнішні сторони, від яких залежить виконання функцій, включно з операційними партнерами), принаймні в разовому порядку.				
219	THIRD-PARTIES-1b	1	Треті сторони, які мають доступ, контроль або зберігання будь-яких IT-активів, OT-активів чи інформаційних активів, які є важливими для виконання функцій, визначаються, принаймні, у певний спосіб.				
220	THIRD-PARTIES-1c	2	Для виявлення ризиків, що виникають від постачальників та інших третіх сторін, використовується певний метод.				
221	THIRD-PARTIES-1d	2	Пріоритетність третіх сторін визначається відповідно до встановлених критеріїв (наприклад, важливість для виконання функції, вплив компромісу чи зриву, здатність обговорювати вимоги кібербезпеки в рамках контрактів).				

1	2	3	4	5	6	7	8
222	THIRD-PARTIES-1e	2	Підвищений пріоритет призначається постачальникам та іншим третім сторонам, компрометація чи збій у яких може спричинити значні наслідки (наприклад, постачальники з одного джерела, постачальники з привілейованим доступом).				
223	THIRD-PARTIES-1f	3	Пріоритезація постачальників та інших третіх сторін періодично оновлюється відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
Ціль 2. Управління ризиками третіх сторін							
224	THIRD-PARTIES-2a	1	Вибір постачальників та інших третіх сторін включає розгляд їхньої кваліфікації з кібербезпеки, принаймні в окремих випадках.				
225	THIRD-PARTIES-2b	1	Вибір продуктів і послуг включає розгляд їхніх можливостей кібербезпеки, принаймні в окремих випадках.				
226	THIRD-PARTIES-2c	2	Використовується окреслений метод для визначення вимог до кібербезпеки та впровадження пов'язаних засобів контролю, які захищають від ризиків, що виникають від постачальників та інших третіх сторін.				
227	THIRD-PARTIES-2d	2	Для оцінки та вибору постачальників та інших третіх осіб використовується визначений метод.				
228	THIRD-PARTIES-2e	2	Для постачальників з вищим пріоритетом та інших третіх сторін реалізовано більш суворий контроль кібербезпеки.				
229	THIRD-PARTIES-2f	2	Вимоги до кібербезпеки (наприклад, повідомлення про вразливості, вимоги SLA (Service Level Agreement договір про рівень обслуговування між замовником та виконавцем послуг), пов'язані з інцидентами) формалізуються в угодах з постачальниками та іншими третіми сторонами.				
230	THIRD-PARTIES-2g	2	Постачальники та інші треті сторони періодично підтверджують свою здатність відповідати вимогам кібербезпеки.				

1	2	3	4	5	6	7	8
231	THIRD-PARTIES-2h	3	Вимоги до кібербезпеки для постачальників та інших третіх сторін включають вимоги до безпечного програмного забезпечення та безпечної розробки продукту, де це необхідно.				
232	THIRD-PARTIES-2i	3	Критерії відбору для продуктів включають розгляд термінів закінчення строку експлуатації та завершення підтримки.				
233	THIRD-PARTIES-2j	3	Критерії відбору включають врахування заходів захисту від підробленого або скомпрометованого програмного забезпечення, обладнання та послуг.				
234	THIRD-PARTIES-2k	3	Критерії відбору для активів з вищим пріоритетом включають оцінку опису матеріалів для ключових елементів активів, таких як апаратне та програмне забезпечення.				
235	THIRD-PARTIES-2l	3	Критерії відбору для активів із вищим пріоритетом включають оцінку будь-яких пов’язаних сторонніх середовищ хостингу та вихідних даних.				
236	THIRD-PARTIES-2m	3	Приймальні випробування закуплених активів включають врахування вимог до кібербезпеки.				
Ціль 3. Управління областю THIRD-PARTIES							
237	THIRD-PARTIES-3a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області THIRD-PARTIES.				
238	THIRD-PARTIES-3b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області THIRD-PARTIES.				
239	THIRD-PARTIES-3c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області THIRD-PARTIES.				
240	THIRD-PARTIES-3d	3	Відповідальність, підзвітність та повноваження щодо здійснення діяльності в області THIRD-PARTIES покладаються на персонал.				

1	2	3	4	5	6	7	8
241	THIRD-PARTIES-3e	3	Персонал, який виконує діяльність у області THIRD-PARTIES, має навички та знання, необхідні для виконання покладених на них обов'язків.				
242	THIRD-PARTIES-3f	3	Ефективність діяльності в області THIRD-PARTIES оцінюється та відстежується.				
Область: Управління персоналом (WORKFORCE)							
Ціль 1. Впровадження засобів контролю персоналу							
243	WORKFORCE-1a	1	Перевірка персоналу (наприклад, перевірка репутації, перевірка на наркотики, тощо) проводиться, принаймні, у тимчасовому порядку.				
244	WORKFORCE-1b	1	Процедури поділу персоналу стосуються кібербезпеки, принаймні в окремих випадках.				
245	WORKFORCE-1c	2	Перевірка персоналу проводиться періодично, принаймні, для посад, які мають доступ до активів, важливих для виконання функцій.				
246	WORKFORCE-1d	2	Процедури поділу та переведення персоналу стосуються кібербезпеки, включаючи додаткову перевірку, якщо це необхідно.				
247	WORKFORCE-1e	2	Персонал поінформований про свою відповідальність за захист і прийнятне використання IT-активів, OT-активів та інформаційних активів.				
248	WORKFORCE-1f	3	Перевірка проводиться для всіх посад (включаючи працівників, постачальників і підрядників) на рівні, відповідному ризику посади.				
249	WORKFORCE-1g	3	Для персоналу, який не дотримується встановлених політик і процедур безпеки, реалізується офіційний процес відповідальності, який включає дисциплінарні заходи.				
Ціль 2. Підвищення обізнаності про кібербезпеку							

1	2	3	4	5	6	7	8
250	WORKFORCE-2a	1	Діяльність з підвищення обізнаності про кібербезпеку відбувається, принаймні, час від часу.				
251	WORKFORCE-2b	2	Цілі щодо обізнаності з кібербезпеки встановлені та підтримуються.				
252	WORKFORCE-2c	2	Цілі поінформованості про кібербезпеку узгоджені з визначеним профілем загроз (практика THREAT-2e).				
253	WORKFORCE-2d	2	Періодично проводяться заходи з підвищення обізнаності щодо кібербезпеки.				
254	WORKFORCE-2e	3	Заходи з підвищення обізнаності щодо кібербезпеки адаптовані до посади.				
255	WORKFORCE-2f	3	Заходи з підвищення обізнаності щодо кібербезпеки стосуються попередньо визначених станів роботи (практика SITUATION-3g).				
256	WORKFORCE-2g	3	Ефективність діяльності з підвищення обізнаності про кібербезпеку оцінюється періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події, і за необхідності вносяться покращення.				
Ціль 3. Розподіл відповідальності за кібербезпеку							
257	WORKFORCE-3a	1	Відповідальність за кібербезпеку визначена, принаймні, в окремих випадках.				
258	WORKFORCE-3b	1	Відповідальність за кібербезпеку покладено на конкретних людей, принаймні в певному порядку.				
259	WORKFORCE-3c	2	Відповідальність за кібербезпеку покладено на певні ролі, зокрема на зовнішніх постачальників послуг.				
260	WORKFORCE-3d	2	Обов'язки щодо кібербезпеки задокументовані.				
261	WORKFORCE-3e	3	Обов'язки щодо кібербезпеки та вимоги до роботи переглядаються та оновлюються періодично та, відповідно, до визначених тригерів, таких як системні зміни та зміни організаційної структури.				

1	2	3	4	5	6	7	8
262	WORKFORCE-3f	3	При призначені обов'язків з кібербезпеки керуються забезпеченням адекватності та надмірності покриття, включаючи правонаступництво планування.				
Ціль 4. Розвиток навичок персоналу з кібербезпеки							
263	WORKFORCE-4a	1	Навчання з кібербезпеки доступне для персоналу, який відповідає за кібербезпеку, принаймні в окремих випадках.				
264	WORKFORCE-4b	1	Вимоги до знань, навичок і здібностей у сфері кібербезпеки, а також прогалини визначаються як для поточних, так і для майбутніх операційних потреб, принаймні в окремих випадках.				
265	WORKFORCE-4c	2	Виявлені прогалини в знаннях, навичках і здібностях у сфері кібербезпеки усуваються шляхом навчання персоналу, додатковому найму фахівців.				
266	WORKFORCE-4d	2	Навчання з кібербезпеки надається як передумова для надання доступу до активів, важливих для виконання функції.				
267	WORKFORCE-4e	3	Ефективність навчальних програм періодично оцінюється, і за необхідності вносяться вдосконалення.				
268	WORKFORCE-4f	3	Програми навчання включають безперервну освіту та можливості професійного розвитку для персоналу, який має значні обов'язки з кібербезпеки.				
Ціль 5. Управління областю WORKFORCE							
269	WORKFORCE-5a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області WORKFORCE.				
270	WORKFORCE-5b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області WORKFORCE.				
271	WORKFORCE-5c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області WORKFORCE.				

1	2	3	4	5	6	7	8
272	WORKFORCE-5d	3	Відповідальність, підзвітність та повноваження щодо виконання діяльності в області WORKFORCE покладаються на персонал.				
273	WORKFORCE-5e	3	Персонал, який виконує діяльність у сфері WORKFORCE, має навички та знання, необхідні для виконання покладених на них обов'язків.				
274	WORKFORCE-5f	3	Ефективність діяльності в області WORKFORCE оцінюється та відстежується.				
Область: Архітектура кібербезпеки (ARCHITECTURE)							
Ціль 1. Створення та підтримка стратегії та програми архітектури кібербезпеки							
275	ARCHITECTURE-1a	1	Організація має стратегію архітектури кібербезпеки, яка розробляється та використовується на практиці час від часу.				
276	ARCHITECTURE-1b	2	Стратегія архітектури кібербезпеки встановлюється та підтримується відповідно до стратегії програми кібербезпеки організації (практика PROGRAM-1b) та архітектури підприємства.				
277	ARCHITECTURE-1c	2	Встановлюється та підтримується задокументована архітектура кібербезпеки, яка включає системи інформаційних, операційних технологій та мережі, і узгоджується з категоризацією та пріоритезацією активів.				
278	ARCHITECTURE-1d	2	Управління архітектурою кібербезпеки (наприклад, процес перевірки архітектури) визначено та підтримується, що включає наявність положення щодо періодичних перевірок архітектури та процесу внесення змін.				
279	ARCHITECTURE-1e	2	Фінансова підтримка вищого керівництва програми архітектури кібербезпеки є помітною і активною.				
280	ARCHITECTURE-1f	2	Архітектура кібербезпеки визначає та підтримує вимоги до кібербезпеки активів організації.				

1	2	3	4	5	6	7	8
281	ARCHITECTURE-1g	2	Засоби керування кібербезпекою вибираються та впроваджуються відповідно до вимог кібербезпеки.				
282	ARCHITECTURE-1h	3	Стратегія та програма архітектури кібербезпеки узгоджені зі стратегією та програмою корпоративної архітектури організації.				
283	ARCHITECTURE-1i	3	Відповідність систем і мереж організації архітектурі кібербезпеки оцінюється періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
284	ARCHITECTURE-1j	3	Архітектура кібербезпеки керується інформацією про аналіз ризиків організації (практика RISK-3d) і профілем загроз (практика THREAT-2e).				
285	ARCHITECTURE-1k	3	Архітектура кібербезпеки посилається на попередньо визначені стани роботи (практика SITUATION-3g).				
Ціль 2. Впровадження захисту мережі як елементу архітектури кібербезпеки							
286	ARCHITECTURE-2a	1	Захист мережі впроваджується, принаймні, у певний спосіб.				
287	ARCHITECTURE-2b	1	Системи інформаційних технологій організації відокремлюються від систем операційних технологій за допомогою сегментації, за допомогою фізичних або логічних засобів, принаймні випадковим чином.				
288	ARCHITECTURE-2c	2	Мережевий захист визначається та забезпечується для вибраних типів активів відповідно до ризику та пріоритету активів (наприклад, внутрішні активи, активи периметра, активи, підключені до Wi-Fi організації, хмарні активи, віддалений доступ і зовнішні пристрої).				
289	ARCHITECTURE-2d	2	Активи, важливі для виконання функції, логічно або фізично сегментуються на окремі зони безпеки відповідно до вимог кібербезпеки активів.				
290	ARCHITECTURE-2e	2	Захист мережі включає принципи найменших привілеїв і найменшої функціональності.				

1	2	3	4	5	6	7	8
291	ARCHITECTURE-2f	2	Захист мережі включає моніторинг, аналіз і контроль мережевого трафіку для вибраних зон безпеки (наприклад, міжмережеві екрани, білі списки, системи виявлення та запобігання вторгненням IDPS).				
292	ARCHITECTURE-2g	2	Веб-трафік і електронна пошта відстежуються, аналізуються та контролюються (наприклад, блокування шкідливих посилань, блокування підозрілих завантажень, методи автентифікації електронної пошти, блокування IP-адрес).				
293	ARCHITECTURE-2h	3	Усі активи сегментовані на окремі зони безпеки відповідно до вимог кібербезпеки.				
294	ARCHITECTURE-2i	3	У разі необхідності реалізуються окремі мережі, які логічно або фізично сегментують активи в зони безпеки з незалежною автентифікацією.				
295	ARCHITECTURE-2j	3	Системи ОТ є операційно незалежними від IT-систем, тому операції ОТ можуть підтримуватися під час збою в роботі IT-систем.				
296	ARCHITECTURE-2k	3	Підключення пристроїв до мережі контролюється, щоб гарантувати підключення лише авторизованих пристроїв (наприклад, контроль доступу до мережі (Network Access Control NAC)).				
297	ARCHITECTURE-2l	3	Архітектура кібербезпеки дозволяє ізолювати скомпрометовані активи.				
Ціль 3. Впровадження безпеки IT-активів та ОТ-активів як елемента архітектури кібербезпеки							
298	ARCHITECTURE-3a	1	Логічний і фізичний контроль доступу впроваджено для захисту активів, важливих для виконання функції, де це можливо, принаймні в окремих випадках.				
299	ARCHITECTURE-3b	1	Захист кінцевих точок (наприклад, безпечна конфігурація, програми безпеки та моніторингу хоста) реалізується для				

1	2	3	4	5	6	7	8
			захисту активів, важливих для виконання функції, де це можливо, принаймні тимчасово.				
300	ARCHITECTURE-3c	2	Застосовується принцип найменших привілеїв (наприклад, обмеження адміністративного доступу для користувачів і облікових записів сервісів).				
301	ARCHITECTURE-3d	2	Застосовується принцип найменшої функціональності (наприклад, обмеження послуг, обмеження програм, обмеження портів, обмеження підключених пристроїв).				
302	ARCHITECTURE-3e	2	Захищені конфігурації встановлюються та підтримуються як частина процесу розгортання активів, де це можливо.				
303	ARCHITECTURE-3f	2	Програми безпеки потрібні як елемент конфігурації пристрою, де це можливо (наприклад, виявлення та реагування на кінцевих точках, міжмережеві екрани на хостах).				
304	ARCHITECTURE-3g	2	Використання знімних носіїв інформації контролюється (наприклад, обмеження використання USB-пристроїв, керування зовнішніми жорсткими дисками).				
305	ARCHITECTURE-3h	2	Контроль кібербезпеки впроваджується для всіх активів у межах функції або на рівні активів, або як компенсаційний контроль, якщо контроль на рівні активів неможливий.				
306	ARCHITECTURE-3i	2	Діяльність з технічного обслуговування та управління потужністю виконується для всіх активів у межах функції.				
307	ARCHITECTURE-3j	2	Фізичне робоче середовище контролюється для захисту роботи активів у межах функції.				
308	ARCHITECTURE-3k	2	Для активів з вищим пріоритетом реалізовано більш суворий контроль кібербезпеки.				
309	ARCHITECTURE-3l	3	Конфігурація та зміни мікропрограм прошивки контролюються протягом життєвого циклу активу.				

1	2	3	4	5	6	7	8
310	ARCHITECTURE-3m	3	Елементи керування (такі як білі списки, чорні списки і налаштування конфігурацій) реалізовано для запобігання виконанню неавторизованого коду.				
Ціль 4. Впровадити безпеку програмного забезпечення як елемент архітектури кібербезпеки							
311	ARCHITECTURE-4a	2	Програмне забезпечення, розроблене власними силами для розгортання на активах з вищим пріоритетом, розробляється з використанням безпечних методів розробки програмного забезпечення.				
312	ARCHITECTURE-4b	2	Вибір закупленого програмного забезпечення для розгортання на активах із вищим пріоритетом включає розгляд практик безпечної розробки програмного забезпечення постачальника.				
313	ARCHITECTURE-4c	2	Захищені конфігурації програмного забезпечення необхідні як частина процесу розгортання програмного забезпечення як для придбаного програмного забезпечення, так і для програмного забезпечення, розробленого власними силами.				
314	ARCHITECTURE-4d	3	Усе програмне забезпечення, розроблене власними силами, розробляється з використанням безпечних методів розробки програмного забезпечення.				
315	ARCHITECTURE-4e	3	Вибір усього закупленого програмного забезпечення включає розгляд практик безпечної розробки програмного забезпечення постачальника.				
316	ARCHITECTURE-4f	3	Процес перегляду архітектури оцінює безпеку нових програм і аналізує програми перед їх розгортанням.				
317	ARCHITECTURE-4g	3	Автентичність усього програмного забезпечення та мікропрограм прошивки перевіряється перед розгортанням.				
318	ARCHITECTURE-4h	3	Тестування безпеки (наприклад, статичне тестування, динамічне тестування, фазинг-тестування, тестування на проникнення) виконується для власно розроблених і власно				

1	2	3	4	5	6	7	8
			спеціально розроблених програм періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
Ціль 5. Впровадити захист даних як елемент архітектури кібербезпеки							
319	ARCHITECTURE-5a	1	Конфіденційні дані захищені в стані спокою, принаймні тимчасово.				
320	ARCHITECTURE-5b	2	Усі дані, що перебувають у стані спокою, захищено для вибраних категорій даних.				
321	ARCHITECTURE-5c	2	Усі дані, що передаються, захищено для вибраних категорій даних.				
322	ARCHITECTURE-5d	2	Для вибраних категорій даних реалізовано засоби криптографічного захисту для даних у стані спокою та даних, що передаються.				
323	ARCHITECTURE-5e	2	Інфраструктура керування ключами (тобто генерація ключів, зберігання ключів, знищення ключів, оновлення ключів і відкликання ключів) реалізована для підтримки криптографічного контролю.				
324	ARCHITECTURE-5f	2	Реалізовано елементи керування для унеможливлення викрадання даних (наприклад, засоби запобігання втраті даних).				
325	ARCHITECTURE-5g	3	Архітектура кібербезпеки включає засоби захисту (наприклад, повне шифрування диска) для даних, які зберігаються на активах, які можуть бути втрачені або викрадені.				
326	ARCHITECTURE-5h	3	Архітектура кібербезпеки включає захист від несанкціонованих змін програмного забезпечення, мікропрограм прошивки обладнання та даних.				
Ціль 6. Управлінська діяльність у сфері ARCHITECTURE							
327	ARCHITECTURE-6a	3	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області ARCHITECTURE.				

1	2	3	4	5	6	7	8
328	ARCHITECTURE-6b	3	Необхідні ресурси (люди, фінансування та інструменти) надаються для підтримки діяльності в області ARCHITECTURE.				
329	ARCHITECTURE-6c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області ARCHITECTURE.				
330	ARCHITECTURE-6d	3	Відповідальність, підзвітність та повноваження щодо здійснення діяльності в області ARCHITECTURE покладаються на персонал.				
331	ARCHITECTURE-6e	3	Персонал, який виконує діяльність в області ARCHITECTURE, має навички та знання, необхідні для виконання покладених на них обов'язків.				
332	ARCHITECTURE-6f	3	Оцінюється та відслідковується ефективність діяльності в області ARCHITECTURE.				
Область: Управління програмою кібербезпеки (PROGRAM)							
Ціль 1. Створення стратегії програми кібербезпеки							
333	PROGRAM-1a	1	Організація має програмну стратегію кібербезпеки, яка може бути розроблена та керована спеціальним чином.				
334	PROGRAM-1b	2	Стратегія програми кібербезпеки визначає цілі та завдання діяльності організації з кібербезпеки.				
335	PROGRAM-1c	2	Стратегія та пріоритети програми кібербезпеки задокументовані та узгоджені з місією організації, стратегічними цілями та ризиками для критичної інфраструктури.				
336	PROGRAM-1d	2	Стратегія програми кібербезпеки визначає підхід організації до забезпечення програмного нагляду та управління діяльністю з кібербезпеки.				
337	PROGRAM-1e	2	Стратегія програми кібербезпеки визначає структуру та організацію програми кібербезпеки.				

1	2	3	4	5	6	7	8
338	PROGRAM-1f	2	Стратегія програми кібербезпеки визначає стандарти та вказівки, яких має дотримуватися програма.				
339	PROGRAM-1g	2	Стратегія програми кібербезпеки визначає будь-які застосовні вимоги відповідності, яким має відповідати програма (наприклад, ISO).				
340	PROGRAM-1h	3	Стратегія програми кібербезпеки оновлюється періодично та відповідно до визначених тригерів, таких як бізнес-зміни, зміни в операційному середовищі та зміни в профілі загроз (практика THREAT-2e).				
Ціль 2. Створення та підтримка програми з кібербезпеки							
341	PROGRAM-2a	1	Вище керівництво з відповідними повноваженнями надає підтримку програмі кібербезпеки, принаймні в окремих випадках.				
342	PROGRAM-2b	2	Програма кібербезпеки створена відповідно до стратегії програми кібербезпеки.				
343	PROGRAM-2c	2	Фінансова підтримка вищого керівництва програми кібербезпеки є помітною і активною.				
344	PROGRAM-2d	2	Фінансова підтримка вищого керівництва надається для розробки, підтримки та забезпечення дотримання політики кібербезпеки.				
345	PROGRAM-2e	2	Відповідальність за програму кібербезпеки покладено на посадову особу із достатніми повноваженнями.				
346	PROGRAM-2f	2	Визначено та залучено зацікавлені сторони для діяльності з управління програмою кібербезпеки.				
347	PROGRAM-2g	3	Діяльність програми кібербезпеки періодично переглядається, щоб переконатися, що вона відповідає стратегії програми кібербезпеки.				
348	PROGRAM-2h	3	Діяльність у сфері кібербезпеки перевіряється незалежно, щоб забезпечити відповідність політикам і процедурам				

1	2	3	4	5	6	7	8
			кібербезпеки, періодично та відповідно до визначених тригерів, таких як зміни процесів.				
349	PROGRAM-2i	3	Програма кібербезпеки спрямована на дотримання законодавчих і нормативних вимог і забезпечує її відповідність.				
350	PROGRAM-2j	3	Організація співпрацює із зовнішніми організаціями, щоб сприяти розробці та впровадженню стандартів кібербезпеки, інструкцій, передових практик, отриманих уроків і нових технологій.				
Ціль 3. Управлінська діяльність для області PROGRAM							
351	PROGRAM-3a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області PROGRAM.				
352	PROGRAM-3b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки заходів в області PROGRAM.				
353	PROGRAM-3c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області PROGRAM.				
354	PROGRAM-3d	3	Відповідальність, підзвітність та повноваження щодо виконання заходів в області PROGRAM покладаються на персонал.				
355	PROGRAM-3e	3	Персонал, який виконує діяльність в області PROGRAM, має навички та знання, необхідні для виконання покладених на них обов'язків.				
356	PROGRAM-3f	3	Оцінюється та відслідковується ефективність діяльності в області PROGRAM.				

Заступник начальника
Управління – начальник відділу
цифрової трансформації Управління
захисту критичної інфраструктури,
кібербезпеки та цифрового розвитку **Віталій БАЗАЛИЦЬКИЙ**

ЗАТВЕРДЖЕНО
Наказ Міністерства енергетики України
«__»_____2024 року № _____

Практики
кібербезпеки електричних мереж

№ з/п	Ідентифікатор практики	MIL	Опис практики	Рівень впровадження			
				NI	PI	LI	FI
1	2	3	4	5	6	7	8
Область: Управління активами, змінами та конфігурацією (ASSET)							
Ціль 1. Управління інвентаризацією IT-активів та OT-активів							
1	ASSET -1a	1	IT-активи та OT-активи, важливі для виконання функції, інвентаризуються, принаймні в певному порядку.				
2	ASSET -1b	2	Інвентаризація IT-активів та OT-активів включає активи в межах функції, які можуть бути використані для досягнення мети загрози.				
3	ASSET -1c	2	Інвентаризовані IT-активи та OT-активи встановлюються за пріоритетністю на основі визначених критеріїв, які включають важливість для виконання функції.				
4	ASSET -1d	2	Критерії визначення пріоритетів включають розгляд ступеня, до якого актив у межах функції може бути використаний для досягнення цілі загрози.				
5	ASSET -1e	2	Інвентаризація IT-активів та OT-активів містить атрибути, які підтримують дії з кібербезпеки (наприклад, розташування, пріоритет активів, власник активів, операційна система та версії прошивки).				

1	2	3	4	5	6	7	8
6	ASSET -1f	3	Інвентаризацію IT-активів та OT-активів завершено (інвентаризація включає всі активи в межах функції).				
7	ASSET -1g	3	Інвентаризація IT-активів та OT-активів є актуальною, тобто періодично оновлюється відповідно до визначених тригерів, наприклад системних змін.				
8	ASSET -1h	3	Дані знищуються або безпечно видаляються з IT-активів та OT-активів перед перерозподілом і в кінці терміну служби.				
Ціль 2. Управління інвентаризацією інформаційних активів							
9	ASSET -2a	1	Інформаційні активи, які є важливими для виконання функції (наприклад, задані значення SCADA та інформація про клієнтів), інвентаризуються, принаймні в певному порядку.				
10	ASSET -2b	2	Інвентаризація інформаційних активів включає інформаційні активи в межах функції, які можуть бути використані для досягнення мети загрози.				
11	ASSET -2c	2	Інвентаризовані інформаційні активи класифікуються на основі визначених критеріїв, які враховують важливість для виконання функції.				
12	ASSET -2d	2	Критерії класифікації враховують розгляд ступеня, до якого інформаційний актив у межах функції може бути використаний для досягнення мети загрози.				
13	ASSET -2e	2	Інвентаризація інформаційних активів включає атрибути, які підтримують дії з кібербезпеки (наприклад, категорія активів, місця та частоту резервного копіювання, місця зберігання, власник активу, вимоги до кібербезпеки).				
14	ASSET -2f	2	Інвентаризація інформаційних активів завершена (інвентаризація включає всі активи в межах функції).				
15	ASSET -2g	2	Інвентаризація інформаційних активів є актуальною, тобто вона оновлюється періодично відповідно до визначених тригерів, таких як системні зміни.				

1	2	3	4	5	6	7	8
16	ASSET -2h	2	Інформаційні активи підлягають санітарній обробці або знищенню наприкінці терміну служби за допомогою методів, які відповідають вимогам кібербезпеки.				
Ціль 3. Управління конфігураціями IT-активів та OT-активів							
17	ASSET -3a	1	Базові параметри конфігурації встановлюються, принаймні, у певний спосіб.				
18	ASSET -3b	2	Базові параметри конфігурації використовуються для налаштування активів під час розгортання та відновлення.				
19	ASSET -3c	2	Базові параметри конфігурації включають відповідні вимоги архітектури кібербезпеки (практика ARCHITECTURE-1f).				
20	ASSET -3d	2	Базові параметри конфігурації періодично переглядаються та оновлюються відповідно до визначених тригерів, таких як системні зміни та зміни в архітектурі кібербезпеки.				
21	ASSET -3e	3	Конфігурації активів перевіряються на узгодженість із базовими протягом усього життєвого циклу активів.				
Ціль 4. Управління змінами в IT-активах та OT-активах							
22	ASSET -4a	1	Зміни в активах оцінюються та затверджуються перед впровадженням, принаймні в окремих випадках.				
23	ASSET -4b	1	Зміни в активах документуються, принаймні в окремих випадках.				
24	ASSET -4c	2	Вимоги до документації щодо змін у активах встановлено та підтримуються.				
25	ASSET -4d	2	Зміни до ресурсів з вищим пріоритетом тестуються перед розгортанням.				
26	ASSET -4e	2	Зміни та оновлення впроваджуються безпечним способом.				
27	ASSET -4f	2	Можливість скасовувати зміни встановлюється та підтримується для активів, які важливі для виконання функції.				

1	2	3	4	5	6	7	8
28	ASSET -4g	2	Практики управління змінами стосуються повного життєвого циклу активів (наприклад, придбання, розгортання, експлуатації та виведення з експлуатації).				
29	ASSET -4h	3	Перед розгортанням зміни в активах з вищим пріоритетом перевіряються на вплив на кібербезпеку.				
30	ASSET -4i	3	Журнали змін містять інформацію про зміни, які впливають на вимоги кібербезпеки активів.				
Ціль 5. Управління областю ASSET							
31	ASSET -5a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області ASSET.				
32	ASSET -5b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області ASSET.				
33	ASSET -5c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області ASSET.				
34	ASSET -5d	3	Відповідальність, підзвітність та повноваження щодо виконання діяльності в області ASSET покладаються на персонал.				
35	ASSET -5e	3	Персонал, який виконує діяльність у області ASSET, має навички та знання, необхідні для виконання покладених на них обов'язків				
36	ASSET -5f	3	Ефективність діяльності в області ASSET оцінюється та відстежується.				
Область: Управління загрозами та вразливостями (THREAT)							
Ціль 1. Зменшення вразливостей кібербезпеки							
37	THREAT-1a	1	Визначаються джерела інформації для підтримки виявлення вразливості кібербезпеки, принаймні в окремих випадках.				
38	THREAT-1b	1	Інформація про вразливість кібербезпеки збирається та інтерпретується для функції, принаймні в окремих випадках.				

1	2	3	4	5	6	7	8
39	THREAT-1c	1	Оцінка вразливості кібербезпеки виконується, принаймні, в разовому порядку.				
40	THREAT-1d	1	Вразливості кібербезпеки, які мають відношення до виконання функції, пом'якшуються, принаймні в окремих випадках.				
41	THREAT-1e	2	Відстежуються джерела інформації про вразливості кібербезпеки, які стосуються активів вищого пріоритету.				
42	THREAT-1f	2	Оцінка вразливості кібербезпеки виконується періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
43	THREAT-1g	2	Виявлені вразливості кібербезпеки аналізуються та встановлюються за пріоритетністю, а також усуваються відповідним чином.				
44	THREAT-1h	2	Операційний вплив на функцію оцінюється перед розгортанням виправлень або інших заходів щодо усунення вразливостей.				
45	THREAT-1i	2	Інформація про виявлені вразливості кібербезпеки передається зацікавленим сторонам, визначеним організацією.				
46	THREAT-1j	3	Відстежуються джерела інформації про вразливості кібербезпеки, які спільно стосуються всіх IT- активів та OT-активів у межах функції.				
47	THREAT-1k	3	Оцінка вразливості кібербезпеки виконується сторонами, які не залежать від операцій цієї функції.				
48	THREAT-1l	3	Діяльність з моніторингу вразливостей включає перевірку, яка підтверджує, що дії, вжиті у відповідь на вразливості кібербезпеки, були ефективними.				
49	THREAT-1m	3	Встановлюються та підтримуються механізми для отримання та реагування на звіти від громадськості чи зовнішніх сторін про потенційну вразливість, пов'язану з IT-активами та OT-активами організації, такими як загальнодоступні веб-сайти або мобільні додатки.				

1	2	3	4	5	6	7	8
Ціль 2. Реагування на загрози та обмін інформацією про загрози							
50	THREAT-2a	1	Внутрішні та зовнішні джерела інформації для підтримки діяльності з управління загрозами визначаються, принаймні в окремих випадках.				
51	THREAT-2b	1	Інформація про загрози кібербезпеці збирається та інтерпретується, принаймні в окремих випадках.				
52	THREAT-2c	1	Цілі щодо загроз для функції визначаються, принаймні, у певний спосіб.				
53	THREAT-2d	1	Загрози, які мають відношення до виконання функції, розглядаються, принаймні, у певний спосіб.				
54	THREAT-2e	2	Встановлюється профіль загрози для функції, який включає цілі загрози та додаткові характеристики загрози (наприклад, типи суб'єктів загрози, мотиви, можливості та цілі).				
55	THREAT-2f	2	Джерела інформації про загрози, які спільно стосуються всіх компонентів профілю загроз, визначаються за пріоритетністю та контролюються.				
56	THREAT-2g	2	Виявлені загрози аналізуються та встановлюються за пріоритетністю, а потім розглядаються відповідно.				
57	THREAT-2h	2	Обмін інформацією про загрози здійснюється із зацікавленими сторонами (наприклад, керівниками, оперативним персоналом, урядом, пов'язаними організаціями, постачальниками, галузевими організаціями, регуляторами, центрами обміну інформацією та аналізу).				
58	THREAT-2i	3	Профіль загроз для функції оновлюється періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
59	THREAT-2j	3	Моніторинг загроз і заходи реагування на них використовують і запускають попередньо визначені стани роботи (практика SITUATION-3g).				

1	2	3	4	5	6	7	8
60	THREAT-2k	3	Захищені методи майже в реальному часі використовуються для отримання та обміну інформацією про загрози, щоб забезпечити швидкий аналіз і дії.				
Ціль 3. Управління областю THREAT							
61	THREAT-3a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області THREAT.				
62	THREAT-3b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області THREAT.				
63	THREAT-3c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області THREAT.				
64	THREAT-3d	3	Відповідальність, підзвітність та повноваження щодо виконання діяльності в області THREAT покладаються на персонал.				
65	THREAT-3e	3	Персонал, який виконує діяльність у області THREAT, має навички та знання, необхідні для виконання покладених на нього обов'язків.				
66	THREAT-3f	3	Оцінюється та відстежується ефективність діяльності в області THREAT.				
Область: Управління ризиками (RISK)							
Ціль 1. Створення та підтримка стратегії та програми управління кіберризиками							
67	RISK-1a	1	Організація має стратегію управління кіберризиками, яка може бути розроблена та керована в індивідуальному порядку.				
68	RISK-1b	2	Стратегія управління кіберризиками створюється та підтримується відповідно до стратегії програми кібербезпеки організації (практика PROGRAM-1b) та архітектури підприємства.				
69	RISK-1c	2	Програма управління кіберризиками створена та підтримується для виконання заходів з управління кіберризиками відповідно до стратегії управління кіберризиками.				

1	2	3	4	5	6	7	8
70	RISK-1d	2	Інформація про діяльність у області RISK передається відповідним зацікавленим сторонам.				
71	RISK-1e	2	Встановлено та підтримується керування програмою управління кіберризиками.				
72	RISK-1f	2	Фінансова підтримка вищого керівництва програми управління кіберризиками є помітною та активною.				
73	RISK-1g	3	Програма управління кіберризиками відповідає місії та цілям організації.				
74	RISK-1h	3	Програма управління кіберризиками узгоджується з загальнокорпоративною програмою управління ризиками організації.				
			Ціль 2. Визначення кіберризиків				
75	RISK-2a	1	Кібернетичні ризики визначаються, принаймні час від часу.				
76	RISK-2b	2	Визначено метод, що використовується для визначення кіберризиків.				
77	RISK-2c	2	Зацікавлені сторони з відповідних операцій і бізнес-сфер беруть участь у виявленні кіберризиків.				
78	RISK-2d	2	Виявлені кіберризики консолідуються за категоріями (наприклад, порушення даних, внутрішні помилки, програми-вимагачі, захоплення контролю), щоб полегшити керування на рівні категорії.				
79	RISK-2e	2	Категорії кіберризиків і кіберризики документуються в реєстрі ризиків або в іншій формі.				
80	RISK-2f	2	Категорії кіберризиків і кіберризики призначаються власникам ризиків.				
81	RISK-2g	2	Діяльність з ідентифікації кіберризиків виконується періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				

1	2	3	4	5	6	7	8
82	RISK-2h	3	Діяльність з ідентифікації кіберризиків використовує інвентаризацію активів та інформацію про пріоритетність із області ASSET, таку як завершення підтримки IT-активів та OT-активів, одиничні точки збою, ризик розкриття, підробки або знищення інформаційних активів.				
83	RISK-2i	3	Інформація про керування вразливістю з області THREAT використовується для оновлення кіберризиків і виявлення нових ризиків (таких як ризики, що виникають через вразливості, які становлять постійний ризик для організації, або нещодавно виявлені вразливості).				
84	RISK-2j	3	Інформація про керування загрозами у області THREAT використовується для оновлення кіберризиків і виявлення нових ризиків.				
85	RISK-2k	3	Інформація про діяльність області THIRD-PARTIES використовується для оновлення кіберризиків і виявлення нових ризиків.				
86	RISK-2l	3	Інформація про дії у області ARCHITECTURE (наприклад, невиправлені прогалини в архітектурі) використовується для оновлення кіберризиків і виявлення нових ризиків.				
87	RISK-2m	3	Ідентифікація кіберризиків враховує ризики, які можуть виникнути або вплинути на інші взаємозалежні організації.				
			Ціль 3. Аналіз кіберризиків				
88	RISK-3a	1	Пріоритезація кіберризиків визначається на основі оцінки їх впливу, принаймні в окремих випадках.				
89	RISK-3b	2	Визначені критерії використовуються для визначення пріоритетності кіберризиків (наприклад, вплив на організацію, вплив на спільноту, ймовірність, сприйнятливість, толерантність до ризику).				

1	2	3	4	5	6	7	8
90	RISK-3c	2	Визначений метод використовується для оцінки впливу кіберризиків з вищим пріоритетом (наприклад, порівняння з реальними подіями, кількісна оцінка ризику).				
91	RISK-3d	2	Визначені методи використовуються для аналізу кіберризиків з вищим пріоритетом (наприклад, аналіз поширеності типів атак для оцінки ймовірності, використання результатів оцінки засобів контролю для оцінки сприйнятливості).				
92	RISK-3e	2	Організаційно зацікавлені сторони з відповідних операцій і бізнес-функцій беруть участь в аналізі кіберризиків з вищим пріоритетом.				
93	RISK-3f	2	Кіберризики видаляються з реєстру ризиків або інших форм їх фіксації, що використовуються для документування виявлених ризиків і керування ними, коли вони більше не потребують відстеження чи реагування.				
94	RISK-3g	3	Аналіз кіберризиків періодично оновлюється відповідно до визначених тригерів, таких як системні зміни, зовнішні події та інформація з інших областей моделі.				
			Ціль 4. Реагування на кіберризики				
95	RISK-4a	1	Реагування на ризики (такі як пом'якшення, прийняття, уникнення або передача) впроваджується для усунення кіберризиків, принаймні в окремих випадках.				
96	RISK-4b	2	Визначений метод використовується для вибору та впровадження заходів реагування на ризики на основі аналізу та встановлення пріоритетів.				
97	RISK-4c	3	Засоби контролю кібербезпеки оцінюються, щоб визначити, чи вони розроблені належним чином і чи функціонують за їх призначенням -для зменшення виявлених кіберризиків.				
98	RISK-4d	3	Результати аналізу впливу кіберризиків і оцінки контролю кібербезпеки разом переглядаються керівництвом				

1	2	3	4	5	6	7	8
			підприємства, щоб визначити, чи достатньо пом'якшено кіберризики та чи не перевищено допустимі рівні ризику.				
99	RISK-4e	3	Реакції на ризики (такі як пом'якшення, прийняття, уникнення або передача) періодично переглядаються керівництвом, щоб визначити, чи вони все ще доцільні.				
Ціль 5. Управління в області RISK							
100	RISK-5a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області RISK.				
101	RISK-5b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області RISK.				
102	RISK-5c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області RISK.				
103	RISK-5d	3	Відповідальність, підзвітність та повноваження щодо виконання діяльності в області RISK покладаються на персонал.				
104	RISK-5e	3	Персонал, який виконує діяльність у області RISK, має навички та знання, необхідні для виконання покладених на них обов'язків.				
105	RISK-5f	3	Оцінюється та відстежується ефективність діяльності в області RISK.				
Область: Управління ідентифікацією та доступом (ACCESS)							
Ціль 1. Встановлення ідентичності та керування автентифікацією							
106	ACCESS-1a	1	Ідентифікаційні дані надаються, принаймні в певному порядку, для персоналу та інших об'єктів, таких як служби та пристрої, яким потрібен доступ до активів (зверніть увагу, що це не виключає спільних ідентифікаційних даних).				
107	ACCESS-1b	1	Облікові дані (такі як паролі, смарт-карти, сертифікати та ключі) видаються персоналу та іншим особам, яким потрібен доступ до активів, принаймні в тимчасовому порядку.				

1	2	3	4	5	6	7	8
108	ACCESS-1c	1	Ідентифікаційні дані деініціалізуються, принаймні тимчасово, коли вони більше не потрібні.				
109	ACCESS-1d	2	Обмеження щодо надійності пароля та повторного його використання визначені та застосовуються.				
110	ACCESS-1e	2	Репозиторії ідентифікаційних даних переглядаються та оновлюються періодично та відповідно до визначених тригерів, таких як системні зміни та зміни організаційної структури.				
111	ACCESS-1f	2	Ідентифікаційні дані деініціалізуються в межах часу, визначеного організацією, коли вони більше не потрібні.				
112	ACCESS-1g	2	Використання привілейованих облікових даних обмежено процесами, для яких вони потрібні.				
113	ACCESS-1h	2	Для доступу з підвищеним ризиком (наприклад, привілейовані облікові записи, облікові записи служб, спільні облікові записи та віддалений доступ) використовуються надійніші облікові дані, багатофакторна автентифікація або одноразові облікові дані.				
114	ACCESS-1i	3	Багатофакторна автентифікація потрібна для будь-якого доступу, де це можливо.				
115	ACCESS-1j	3	Ідентифікаційні дані вимикаються після певного періоду бездіяльності, де це можливо.				
			Ціль 2. Контроль логічного доступу				
116	ACCESS-2a	1	Реалізовано логічний контроль доступу, принаймні, у певний спосіб.				
117	ACCESS-2b	1	Привілеї логічного доступу скасовуються, коли більше не потрібні, принаймні інколи.				
118	ACCESS-2c	2	Встановлюються та підтримуються вимоги до логічного доступу (наприклад, правила, яким типам об’єктів дозволено доступ до активу, обмеження дозволеного доступу, обмеження віддаленого доступу, параметри автентифікації).				

1	2	3	4	5	6	7	8
119	ACCESS-2d	2	Вимоги до логічного доступу включають принцип найменших привілеїв.				
120	ACCESS-2e	2	Вимоги до логічного доступу включають принцип розподілу обов'язків.				
121	ACCESS-2f	2	Запити на логічний доступ переглядаються та затверджуються власником ресурсу.				
122	ACCESS-2g	2	Привілеї логічного доступу, які становлять більший ризик для функції, отримують додаткову перевірку та моніторинг.				
123	ACCESS-2h	3	Логічні привілеї доступу переглядаються та оновлюються для забезпечення відповідності вимогам доступу періодично та відповідно до визначених тригерів, таких як зміни в організаційній структурі, і після будь-якого тимчасового підвищення привілеїв.				
124	ACCESS-2i	3	Аномальні спроби отримати логічний доступ відстежуються як індикатори подій кібербезпеки.				
			Ціль 3. Контроль фізичного доступу				
125	ACCESS-3a	1	Фізичні засоби контролю доступу (такі як огорожі, замки та вивіски) реалізовані, принаймні в певному порядку.				
126	ACCESS-3b	1	Привілеї фізичного доступу скасовуються, коли вони більше не потрібні, принаймні інколи.				
127	ACCESS-3c	1	Журнали фізичного доступу зберігаються, принаймні в певному порядку.				
128	ACCESS-3d	2	Вимоги до фізичного доступу встановлюються та підтримуються (наприклад, правила щодо того, хто має доступ до активу, як надається доступ, обмеження дозволеного доступу).				
129	ACCESS-3e	2	Вимоги щодо фізичного доступу включають принцип найменших привілеїв.				

1	2	3	4	5	6	7	8
130	ACCESS-3f	2	Вимоги щодо фізичного доступу включають принцип розподілу обов'язків.				
131	ACCESS-3g	2	Запити на фізичний доступ розглядаються та затверджуються власником ресурсу.				
132	ACCESS-3h	2	Привілеї фізичного доступу, які створюють підвищений ризик для функції, отримують додаткову перевірку та моніторинг.				
133	ACCESS-3i	3	Привілеї фізичного доступу переглядаються та оновлюються.				
134	ACCESS-3j	3	Фізичний доступ відстежується для виявлення потенційних подій кібербезпеки.				
Ціль 4. Управління в області ACCESS							
135	ACCESS-4a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області ACCESS.				
136	ACCESS-4b	2	Для підтримки діяльності в області ACCESS надаються відповідні ресурси (люди, фінансування та інструменти).				
137	ACCESS-4c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області ACCESS.				
138	ACCESS-4d	3	Відповідальність, підзвітність та повноваження щодо виконання діяльності в області ACCESS покладаються на персонал.				
139	ACCESS-4e	3	Персонал, який виконує діяльність у області ACCESS, має навички та знання, необхідні для виконання покладених на них обов'язків.				
140	ACCESS-4f	3	Ефективність діяльності в області ACCESS оцінюється та відстежується.				
Область: Ситуаційна обізнаність (SITUATION)							
Ціль 1. Виконання журналювання							
141	SITUATION -1a	1	Реєстрація ведеться для активів, які важливі для виконання функції, принаймні одноразово.				

1	2	3	4	5	6	7	8
142	SITUATION-1b	2	Журналювання проводиться де це можливо для активів у операціях, які можуть бути використані для досягнення мети загрози.				
143	SITUATION-1c	2	Вимоги до журналювання встановлюються та підтримуються для IT-активів та OT-активів, важливих для виконання функції, і активів у межах функції, які можуть бути використані для досягнення цілі загрози.				
144	SITUATION-1d	2	Вимоги до журналювання встановлюються та підтримуються для інфраструктури моніторингу мережі та хостів (наприклад, веб-шлюзи, програмне забезпечення для виявлення і реагування на кінцевих точках, системи виявлення та запобігання вторгненням).				
145	SITUATION-1e	2	Дані журналу агрегуються у межах функції.				
146	SITUATION-1f	3	Ретельніше журналювання виконується для активів з вищим пріоритетом.				
			Ціль 2. Проведення моніторингу				
147	SITUATION-2a	1	Виконуються періодичні перевірки даних журналів або інші заходи моніторингу кібербезпеки, принаймні в разовому порядку.				
148	SITUATION-2b	1	Дані та сповіщення з мережевих і хост-моніторингових активів інфраструктури періодично переглядаються, принаймні в разовому порядку.				
149	SITUATION-2c	2	Вимоги до моніторингу та аналізу встановлюються та підтримуються для функції та забезпечують своєчасний перегляд даних про події.				
150	SITUATION-2d	2	Індикатори аномальної активності встановлюються та підтримуються на основі системних журналів, потоків даних, базових показників мережі, подій кібербезпеки та архітектури				

1	2	3	4	5	6	7	8
			та відстежуються в середовищах як інформаційних так операційних технологій.				
151	SITUATION-2e	2	Сигнали тривоги та сповіщення налаштовані та підтримуються для підтримки ідентифікації подій кібербезпеки.				
152	SITUATION-2f	2	Діяльність моніторингу узгоджується з профілем загроз (практика THREAT-2e).				
153	SITUATION-2g	3	Ретельніший моніторинг здійснюється для активів з вищим пріоритетом.				
154	SITUATION-2h	3	Інформація аналізу ризиків (практика RISK-3d) використовується для визначення показників аномальної активності.				
155	SITUATION-2i	3	Індикатори аномальної активності оцінюються та оновлюються періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
Ціль 3. Створення та підтримка обізнаності про ситуацію							
156	SITUATION-3a	2	Методи передачі інформації про поточний стан кібербезпеки для функції встановлено та підтримуються.				
157	SITUATION-3b	2	Дані моніторингу агрегируються, щоб забезпечити розуміння робочого стану функції.				
158	SITUATION-3c	2	Відповідна інформація з усієї організації доступна для підвищення обізнаності про ситуацію.				
159	SITUATION-3d	3	Було визначено вимоги до звітності щодо обізнаності про ситуацію, які стосуються своєчасного розповсюдження інформації про кібербезпеку зацікавленим сторонам, визначеним організацією.				
160	SITUATION-3e	3	Релевантна інформація ззовні організації збирається та стає доступною в усій організації для підвищення обізнаності про ситуацію.				

1	2	3	4	5	6	7	8
161	SITUATION-3f	3	Встановлено та підтримується можливість агрегирувати, співвідносити та аналізувати результати діяльності моніторингу кібербезпеки та надавати майже в реальному часі розуміння стану кібербезпеки функції.				
162	SITUATION-3g	3	Попередньо визначені стани роботи задокументовані та можуть бути реалізовані на основі стану кібербезпеки функції або коли вони викликані діяльністю в інших областях.				
Ціль 4. Управління у області SITUATION							
163	SITUATION-4a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області SITUATION.				
164	SITUATION-4b	2	Достатні ресурси (люди, фінансування та інструменти) надаються для підтримки діяльності в області SITUATION.				
165	SITUATION-4c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області SITUATION.				
166	SITUATION-4d	3	Відповідальність, підзвітність та повноваження щодо виконання заходів у області SITUATION покладаються на персонал.				
167	SITUATION-4e	3	Персонал, який виконує діяльність у області SITUATION, має навички та знання, необхідні для виконання покладених на нього обов'язків.				
168	SITUATION-4f	3	Оцінюється та відстежується ефективність діяльності в області SITUATION.				
Область: Реагування на події та інциденти, безперервність роботи (RESPONSE)							
Ціль 1. Виявлення події кібербезпеки							
169	RESPONSE-1a	1	Виявлені події кібербезпеки повідомляються певній особі або ролі та документуються, принаймні в певному порядку.				
170	RESPONSE-1b	2	Встановлюються критерії для виявлення подій кібербезпеки (наприклад, що є подією кібербезпеки, де шукати події кібербезпеки).				

1	2	3	4	5	6	7	8
171	RESPONSE-1c	2	Події кібербезпеки документуються на основі встановлених критеріїв.				
172	RESPONSE-1d	3	Інформація про події корелюється для підтримки аналізу інцидентів шляхом виявлення закономірностей, тенденцій та інших загальних характеристик.				
173	RESPONSE-1e	3	Діяльність виявлення подій кібербезпеки коригується на основі виявлених ризиків і профілю загрози організації (практика THREAT-2e).				
174	RESPONSE-1f	3	Ситуаційна обізнаність для функції контролюється для підтримки ідентифікації подій кібербезпеки.				
Ціль 2. Аналіз подій кібербезпеки та оголошення про інциденти							
175	RESPONSE-2a	1	Критерії для оголошення інцидентів кібербезпеки встановлюються, принаймні в окремих випадках.				
176	RESPONSE-2b	1	Події кібербезпеки аналізуються, щоб підтвердити декларування про інциденти кібербезпеки, принаймні в окремих випадках.				
177	RESPONSE-2c	2	Критерії декларування інцидентів кібербезпеки формально встановлюються на основі потенційного впливу на функцію.				
178	RESPONSE-2d	2	Події кібербезпеки оголошуються інцидентами на основі встановлених критеріїв.				
179	RESPONSE-2e	2	Критерії декларування інцидентів кібербезпеки періодично оновлюються відповідно до визначених тригерів, таких як організаційні зміни, висновки, отримані під час виконання плану з кіберзахисту, або нещодавно виявлені загрози.				
180	RESPONSE-2f	2	Є репозиторій, де події та інциденти кібербезпеки документуються та відстежуються до закриття.				
181	RESPONSE-2g	2	Внутрішні та зовнішні зацікавлені сторони (наприклад, керівники, юристи, державні установи, пов'язані організації, постачальники, галузеві організації, регулятори) визначаються				

1	2	3	4	5	6	7	8
			та повідомляються про інциденти на основі вимог щодо звітності про ситуацію (практика SITUATION-3d).				
182	RESPONSE-2h	3	Критерії для декларування інцидентів кібербезпеки узгоджені з критеріями пріоритетності кіберризиків (практика RISK-3b).				
183	RESPONSE-2i	3	Інциденти кібербезпеки порівнюються, аналізуються, щоб визначити закономірності, тенденції та інші загальні характеристики в кількох інцидентах.				
Ціль 3. Реагування на інциденти кібербезпеки							
184	RESPONSE-3a	1	Визначається персонал задіяний у реагуванні на інциденти кібербезпеки та розподіляються ролі, принаймні в окремих випадках.				
185	RESPONSE-3b	1	Реагування на інциденти кібербезпеки виконується, принаймні, у певний спосіб, щоб обмежити вплив на функцію та відновити нормальну роботу.				
186	RESPONSE-3c	1	Звітування про інциденти здійснюється (наприклад, внутрішня звітність, CERT-UA, тощо), принаймні в разовому порядку.				
187	RESPONSE-3d	2	Розробляються та підтримуються плани реагування на інциденти кібербезпеки, які стосуються всіх етапів життєвого циклу інциденту.				
188	RESPONSE-3e	2	Реагування на інциденти кібербезпеки виконується відповідно до визначених планів і процедур.				
189	RESPONSE-3f	2	Плани реагування на інциденти кібербезпеки включають план комунікацій для внутрішніх і зовнішніх зацікавлених сторін.				
190	RESPONSE-3g	2	Навчання плану реагування на інциденти кібербезпеки проводяться періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
191	RESPONSE-3h	2	Виконуються заходи на основі отриманих уроків щодо інцидентів кібербезпеки та вживаються коригувальні дії, включаючи оновлення плану реагування на інциденти.				

1	2	3	4	5	6	7	8
192	RESPONSE-3i	3	Виконується аналіз основних причин інциденту кібербезпеки та вживаються коригувальні дії, включаючи оновлення плану реагування на інциденти.				
193	RESPONSE-3j	3	Реагування на інциденти кібербезпеки узгоджується з постачальниками, правоохоронними органами та іншими зовнішніми організаціями, якщо це необхідно, включаючи підтримку збору та збереження доказів.				
194	RESPONSE-3k	3	Персонал з реагування на інциденти кібербезпеки бере участь у спільних навчаннях з кібербезпеки з іншими організаціями.				
195	RESPONSE-3l	3	Реагування на інциденти кібербезпеки використовує та запускає попередньо визначені режими роботи (практика SITUATION-3g).				
Ціль 4. Вирішення проблеми кібербезпеки в безперервності операцій							
196	RESPONSE-4a	1	Розробляються плани безперервності, щоб підтримувати та відновлювати роботу функції, якщо трапляється подія чи інцидент у сфері кібербезпеки, принаймні випадково.				
197	RESPONSE-4b	1	Резервне копіювання даних доступне та протестоване, принаймні в разовому порядку.				
198	RESPONSE-4c	1	IT-активи та OT-активи, які потребують запасних частин, визначаються, принаймні, в окремих випадках.				
199	RESPONSE-4d	2	У планах забезпечення безперервності розглядаються потенційні наслідки інцидентів кібербезпеки.				
200	RESPONSE-4e	2	Активи та діяльність, необхідні для підтримки мінімальних операцій функції, визначаються та документуються в планах безперервності.				
201	RESPONSE-4f	2	Плани забезпечення безперервності стосуються IT-активів, OT-активів та інформаційних активів, які важливі для виконання функцій, включаючи наявність резервних копій даних і їх заміни, надлишкових та резервних IT-активів і OT-активів.				

1	2	3	4	5	6	7	8
202	RESPONSE-4g	2	Цільові показники часу відновлення (RTO) і точки відновлення (RPO) для активів, які важливі для виконання функції, включені до планів безперервності.				
203	RESPONSE-4h	2	Критерії інциденту кібербезпеки, які ініціюють виконання планів безперервності, встановлюються та повідомляються персоналу з реагування на інциденти та управління безперервністю.				
204	RESPONSE-4i	2	Плани безперервності перевіряються за допомогою оцінювання та періодичних вправ відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
205	RESPONSE-4j	2	Контроль кібербезпеки, що захищає резервні дані, еквівалентний або більш суворий, ніж контроль, що захищає вихідні дані.				
206	RESPONSE-4k	2	Резервні копії даних логічно або фізично відокремлені від вихідних даних.				
207	RESPONSE-4l	2	Доступні запчастини для вибраних IT- та OT-активів.				
208	RESPONSE-4m	3	Плани безперервності узгоджені з виявленими ризиками та профілем загроз організації (практика THREAT-2e), щоб забезпечити покриття визначених категорій ризиків і загроз.				
209	RESPONSE-4n	3	Навчання плану безперервності стосуються ризиків вищого пріоритету.				
210	RESPONSE-4o	3	Результати тестування або активації плану безперервності порівнюються з цілями відновлення, і плани відповідно вдосконалюються.				
211	RESPONSE-4p	3	Плани безперервності періодично переглядаються та оновлюються.				
Ціль 5. Управління областю RESPONSE							
212	RESPONSE-5a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області RESPONSE.				

1	2	3	4	5	6	7	8
213	RESPONSE-5b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області RESPONSE.				
214	RESPONSE-5c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області RESPONSE.				
215	RESPONSE-5d	3	Відповідальність, підзвітність та повноваження щодо здійснення діяльності у області RESPONSE покладено на персонал.				
216	RESPONSE-5e	3	Персонал, який виконує діяльність у області RESPONSE, має навички та знання, необхідні для виконання покладених на них обов'язків.				
217	RESPONSE-5f	3	Оцінюється та відстежується ефективність діяльності в області RESPONSE.				
Область: Управління ланцюгами постачання та зовнішніми взаємозалежностями (THIRD-PARTIES)							
Ціль 1. Виявлення третіх сторін і визначення пріоритетів							
218	THIRD-PARTIES-1a	1	Визначаються важливі залежності інформаційних та операційних технологій від третіх сторін (тобто внутрішні та зовнішні сторони, від яких залежить виконання функцій, включно з операційними партнерами), принаймні в разовому порядку.				
219	THIRD-PARTIES-1b	1	Треті сторони, які мають доступ, контроль або зберігання будь-яких IT-активів, OT-активів чи інформаційних активів, які є важливими для виконання функцій, визначаються, принаймні, у певний спосіб.				
220	THIRD-PARTIES-1c	2	Для виявлення ризиків, що виникають від постачальників та інших третіх сторін, використовується певний метод.				
221	THIRD-PARTIES-1d	2	Пріоритетність третіх сторін визначається відповідно до встановлених критеріїв (наприклад, важливість для виконання функції, вплив компромісу чи зриву, здатність обговорювати вимоги кібербезпеки в рамках контрактів).				

1	2	3	4	5	6	7	8
222	THIRD-PARTIES-1e	2	Підвищений пріоритет призначається постачальникам та іншим третім сторонам, компрометація чи збій у яких може спричинити значні наслідки (наприклад, постачальники з одного джерела, постачальники з привілейованим доступом).				
223	THIRD-PARTIES-1f	3	Пріоритезація постачальників та інших третіх сторін періодично оновлюється відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
Ціль 2. Управління ризиками третіх сторін							
224	THIRD-PARTIES-2a	1	Вибір постачальників та інших третіх сторін включає розгляд їхньої кваліфікації з кібербезпеки, принаймні в окремих випадках.				
225	THIRD-PARTIES-2b	1	Вибір продуктів і послуг включає розгляд їхніх можливостей кібербезпеки, принаймні в окремих випадках.				
226	THIRD-PARTIES-2c	2	Використовується окреслений метод для визначення вимог до кібербезпеки та впровадження пов'язаних засобів контролю, які захищають від ризиків, що виникають від постачальників та інших третіх сторін.				
227	THIRD-PARTIES-2d	2	Для оцінки та вибору постачальників та інших третіх осіб використовується визначений метод.				
228	THIRD-PARTIES-2e	2	Для постачальників з вищим пріоритетом та інших третіх сторін реалізовано більш суворий контроль кібербезпеки.				
229	THIRD-PARTIES-2f	2	Вимоги до кібербезпеки (наприклад, повідомлення про вразливості, вимоги SLA (Service Level Agreement договір про рівень обслуговування між замовником та виконавцем послуг), пов'язані з інцидентами) формалізуються в угодах з постачальниками та іншими третіми сторонами.				
230	THIRD-PARTIES-2g	2	Постачальники та інші треті сторони періодично підтверджують свою здатність відповідати вимогам кібербезпеки.				

1	2	3	4	5	6	7	8
231	THIRD-PARTIES-2h	3	Вимоги до кібербезпеки для постачальників та інших третіх сторін включають вимоги до безпечного програмного забезпечення та безпечної розробки продукту, де це необхідно.				
232	THIRD-PARTIES-2i	3	Критерії відбору для продуктів включають розгляд термінів закінчення строку експлуатації та завершення підтримки.				
233	THIRD-PARTIES-2j	3	Критерії відбору включають врахування заходів захисту від підробленого або скомпрометованого програмного забезпечення, обладнання та послуг.				
234	THIRD-PARTIES-2k	3	Критерії відбору для активів з вищим пріоритетом включають оцінку опису матеріалів для ключових елементів активів, таких як апаратне та програмне забезпечення.				
235	THIRD-PARTIES-2l	3	Критерії відбору для активів із вищим пріоритетом включають оцінку будь-яких пов’язаних сторонніх середовищ хостингу та вихідних даних.				
236	THIRD-PARTIES-2m	3	Приймальні випробування закуплених активів включають врахування вимог до кібербезпеки.				
Ціль 3. Управління областю THIRD-PARTIES							
237	THIRD-PARTIES-3a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області THIRD-PARTIES.				
238	THIRD-PARTIES-3b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області THIRD-PARTIES.				
239	THIRD-PARTIES-3c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області THIRD-PARTIES.				
240	THIRD-PARTIES-3d	3	Відповідальність, підзвітність та повноваження щодо здійснення діяльності в області THIRD-PARTIES покладаються на персонал.				

1	2	3	4	5	6	7	8
241	THIRD-PARTIES-3e	3	Персонал, який виконує діяльність у області THIRD-PARTIES, має навички та знання, необхідні для виконання покладених на них обов'язків.				
242	THIRD-PARTIES-3f	3	Ефективність діяльності в області THIRD-PARTIES оцінюється та відстежується.				
Область: Управління персоналом (WORKFORCE)							
Ціль 1. Впровадження засобів контролю персоналу							
243	WORKFORCE-1a	1	Перевірка персоналу (наприклад, перевірка репутації, перевірка на наркотики, тощо) проводиться, принаймні, у тимчасовому порядку.				
244	WORKFORCE-1b	1	Процедури поділу персоналу стосуються кібербезпеки, принаймні в окремих випадках.				
245	WORKFORCE-1c	2	Перевірка персоналу проводиться періодично, принаймні, для посад, які мають доступ до активів, важливих для виконання функцій.				
246	WORKFORCE-1d	2	Процедури поділу та переведення персоналу стосуються кібербезпеки, включаючи додаткову перевірку, якщо це необхідно.				
247	WORKFORCE-1e	2	Персонал поінформований про свою відповідальність за захист і прийнятне використання IT-активів, OT-активів та інформаційних активів.				
248	WORKFORCE-1f	3	Перевірка проводиться для всіх посад (включаючи працівників, постачальників і підрядників) на рівні, відповідному ризику посади.				
249	WORKFORCE-1g	3	Для персоналу, який не дотримується встановлених політик і процедур безпеки, реалізується офіційний процес відповідальності, який включає дисциплінарні заходи.				
Ціль 2. Підвищення обізнаності про кібербезпеку							

1	2	3	4	5	6	7	8
250	WORKFORCE-2a	1	Діяльність з підвищення обізнаності про кібербезпеку відбувається, принаймні, час від часу.				
251	WORKFORCE-2b	2	Цілі щодо обізнаності з кібербезпеки встановлені та підтримуються.				
252	WORKFORCE-2c	2	Цілі поінформованості про кібербезпеку узгоджені з визначеним профілем загроз (практика THREAT-2e).				
253	WORKFORCE-2d	2	Періодично проводяться заходи з підвищення обізнаності щодо кібербезпеки.				
254	WORKFORCE-2e	3	Заходи з підвищення обізнаності щодо кібербезпеки адаптовані до посади.				
255	WORKFORCE-2f	3	Заходи з підвищення обізнаності щодо кібербезпеки стосуються попередньо визначених станів роботи (практика SITUATION-3g).				
256	WORKFORCE-2g	3	Ефективність діяльності з підвищення обізнаності про кібербезпеку оцінюється періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події, і за необхідності вносяться покращення.				
Ціль 3. Розподіл відповідальності за кібербезпеку							
257	WORKFORCE-3a	1	Відповідальність за кібербезпеку визначена, принаймні, в окремих випадках.				
258	WORKFORCE-3b	1	Відповідальність за кібербезпеку покладено на конкретних людей, принаймні в певному порядку.				
259	WORKFORCE-3c	2	Відповідальність за кібербезпеку покладено на певні ролі, зокрема на зовнішніх постачальників послуг.				
260	WORKFORCE-3d	2	Обов'язки щодо кібербезпеки задокументовані.				
261	WORKFORCE-3e	3	Обов'язки щодо кібербезпеки та вимоги до роботи переглядаються та оновлюються періодично та, відповідно, до визначених тригерів, таких як системні зміни та зміни організаційної структури.				

1	2	3	4	5	6	7	8
262	WORKFORCE-3f	3	При призначені обов'язків з кібербезпеки керуються забезпеченням адекватності та надмірності покриття, включаючи правонаступництво планування.				
Ціль 4. Розвиток навичок персоналу з кібербезпеки							
263	WORKFORCE-4a	1	Навчання з кібербезпеки доступне для персоналу, який відповідає за кібербезпеку, принаймні в окремих випадках.				
264	WORKFORCE-4b	1	Вимоги до знань, навичок і здібностей у сфері кібербезпеки, а також прогалини визначаються як для поточних, так і для майбутніх операційних потреб, принаймні в окремих випадках.				
265	WORKFORCE-4c	2	Виявлені прогалини в знаннях, навичках і здібностях у сфері кібербезпеки усуваються шляхом навчання персоналу, додатковому найму фахівців.				
266	WORKFORCE-4d	2	Навчання з кібербезпеки надається як передумова для надання доступу до активів, важливих для виконання функції.				
267	WORKFORCE-4e	3	Ефективність навчальних програм періодично оцінюється, і за необхідності вносяться вдосконалення.				
268	WORKFORCE-4f	3	Програми навчання включають безперервну освіту та можливості професійного розвитку для персоналу, який має значні обов'язки з кібербезпеки.				
Ціль 5. Управління областю WORKFORCE							
269	WORKFORCE-5a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області WORKFORCE.				
270	WORKFORCE-5b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки діяльності в області WORKFORCE.				
271	WORKFORCE-5c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області WORKFORCE.				

1	2	3	4	5	6	7	8
272	WORKFORCE-5d	3	Відповідальність, підзвітність та повноваження щодо виконання діяльності в області WORKFORCE покладаються на персонал.				
273	WORKFORCE-5e	3	Персонал, який виконує діяльність у сфері WORKFORCE, має навички та знання, необхідні для виконання покладених на них обов'язків.				
274	WORKFORCE-5f	3	Ефективність діяльності в області WORKFORCE оцінюється та відстежується.				
Область: Архітектура кібербезпеки (ARCHITECTURE)							
Ціль 1. Створення та підтримка стратегії та програми архітектури кібербезпеки							
275	ARCHITECTURE-1a	1	Організація має стратегію архітектури кібербезпеки, яка розробляється та використовується на практиці час від часу.				
276	ARCHITECTURE-1b	2	Стратегія архітектури кібербезпеки встановлюється та підтримується відповідно до стратегії програми кібербезпеки організації (практика PROGRAM-1b) та архітектури підприємства.				
277	ARCHITECTURE-1c	2	Встановлюється та підтримується задокументована архітектура кібербезпеки, яка включає системи інформаційних, операційних технологій та мережі, і узгоджується з категоризацією та пріоритезацією активів.				
278	ARCHITECTURE-1d	2	Управління архітектурою кібербезпеки (наприклад, процес перевірки архітектури) визначено та підтримується, що включає наявність положення щодо періодичних перевірок архітектури та процесу внесення змін.				
279	ARCHITECTURE-1e	2	Фінансова підтримка вищого керівництва програми архітектури кібербезпеки є помітною і активною.				
280	ARCHITECTURE-1f	2	Архітектура кібербезпеки визначає та підтримує вимоги до кібербезпеки активів організації.				

1	2	3	4	5	6	7	8
281	ARCHITECTURE-1g	2	Засоби керування кібербезпекою вибираються та впроваджуються відповідно до вимог кібербезпеки.				
282	ARCHITECTURE-1h	3	Стратегія та програма архітектури кібербезпеки узгоджені зі стратегією та програмою корпоративної архітектури організації.				
283	ARCHITECTURE-1i	3	Відповідність систем і мереж організації архітектурі кібербезпеки оцінюється періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
284	ARCHITECTURE-1j	3	Архітектура кібербезпеки керується інформацією про аналіз ризиків організації (практика RISK-3d) і профілем загроз (практика THREAT-2e).				
285	ARCHITECTURE-1k	3	Архітектура кібербезпеки посилається на попередньо визначені стани роботи (практика SITUATION-3g).				
Ціль 2. Впровадження захисту мережі як елементу архітектури кібербезпеки							
286	ARCHITECTURE-2a	1	Захист мережі впроваджується, принаймні, у певний спосіб.				
287	ARCHITECTURE-2b	1	Системи інформаційних технологій організації відокремлюються від систем операційних технологій за допомогою сегментації, за допомогою фізичних або логічних засобів, принаймні випадковим чином.				
288	ARCHITECTURE-2c	2	Мережевий захист визначається та забезпечується для вибраних типів активів відповідно до ризику та пріоритету активів (наприклад, внутрішні активи, активи периметра, активи, підключені до Wi-Fi організації, хмарні активи, віддалений доступ і зовнішні пристрої).				
289	ARCHITECTURE-2d	2	Активи, важливі для виконання функції, логічно або фізично сегментуються на окремі зони безпеки відповідно до вимог кібербезпеки активів.				
290	ARCHITECTURE-2e	2	Захист мережі включає принципи найменших привілеїв і найменшої функціональності.				

1	2	3	4	5	6	7	8
291	ARCHITECTURE-2f	2	Захист мережі включає моніторинг, аналіз і контроль мережевого трафіку для вибраних зон безпеки (наприклад, міжмережеві екрани, білі списки, системи виявлення та запобігання вторгненням IDPS).				
292	ARCHITECTURE-2g	2	Веб-трафік і електронна пошта відстежуються, аналізуються та контролюються (наприклад, блокування шкідливих посилань, блокування підозрілих завантажень, методи автентифікації електронної пошти, блокування IP-адрес).				
293	ARCHITECTURE-2h	3	Усі активи сегментовані на окремі зони безпеки відповідно до вимог кібербезпеки.				
294	ARCHITECTURE-2i	3	У разі необхідності реалізуються окремі мережі, які логічно або фізично сегментують активи в зони безпеки з незалежною автентифікацією.				
295	ARCHITECTURE-2j	3	Системи ОТ є операційно незалежними від IT-систем, тому операції ОТ можуть підтримуватися під час збою в роботі IT-систем.				
296	ARCHITECTURE-2k	3	Підключення пристроїв до мережі контролюється, щоб гарантувати підключення лише авторизованих пристроїв (наприклад, контроль доступу до мережі (Network Access Control NAC)).				
297	ARCHITECTURE-2l	3	Архітектура кібербезпеки дозволяє ізолювати скомпрометовані активи.				
Ціль 3. Впровадження безпеки IT-активів та ОТ-активів як елемента архітектури кібербезпеки							
298	ARCHITECTURE-3a	1	Логічний і фізичний контроль доступу впроваджено для захисту активів, важливих для виконання функції, де це можливо, принаймні в окремих випадках.				
299	ARCHITECTURE-3b	1	Захист кінцевих точок (наприклад, безпечна конфігурація, програми безпеки та моніторингу хоста) реалізується для				

1	2	3	4	5	6	7	8
			захисту активів, важливих для виконання функції, де це можливо, принаймні тимчасово.				
300	ARCHITECTURE-3c	2	Застосовується принцип найменших привілеїв (наприклад, обмеження адміністративного доступу для користувачів і облікових записів сервісів).				
301	ARCHITECTURE-3d	2	Застосовується принцип найменшої функціональності (наприклад, обмеження послуг, обмеження програм, обмеження портів, обмеження підключених пристроїв).				
302	ARCHITECTURE-3e	2	Захищені конфігурації встановлюються та підтримуються як частина процесу розгортання активів, де це можливо.				
303	ARCHITECTURE-3f	2	Програми безпеки потрібні як елемент конфігурації пристрою, де це можливо (наприклад, виявлення та реагування на кінцевих точках, міжмережеві екрани на хостах).				
304	ARCHITECTURE-3g	2	Використання знімних носіїв інформації контролюється (наприклад, обмеження використання USB-пристроїв, керування зовнішніми жорсткими дисками).				
305	ARCHITECTURE-3h	2	Контроль кібербезпеки впроваджується для всіх активів у межах функції або на рівні активів, або як компенсаційний контроль, якщо контроль на рівні активів неможливий.				
306	ARCHITECTURE-3i	2	Діяльність з технічного обслуговування та управління потужністю виконується для всіх активів у межах функції.				
307	ARCHITECTURE-3j	2	Фізичне робоче середовище контролюється для захисту роботи активів у межах функції.				
308	ARCHITECTURE-3k	2	Для активів з вищим пріоритетом реалізовано більш суворий контроль кібербезпеки.				
309	ARCHITECTURE-3l	3	Конфігурація та зміни мікропрограм прошивки контролюються протягом життєвого циклу активу.				

1	2	3	4	5	6	7	8
310	ARCHITECTURE-3m	3	Елементи керування (такі як білі списки, чорні списки і налаштування конфігурацій) реалізовано для запобігання виконанню неавторизованого коду.				
Ціль 4. Впровадити безпеку програмного забезпечення як елемент архітектури кібербезпеки							
311	ARCHITECTURE-4a	2	Програмне забезпечення, розроблене власними силами для розгортання на активах з вищим пріоритетом, розробляється з використанням безпечних методів розробки програмного забезпечення.				
312	ARCHITECTURE-4b	2	Вибір закупленого програмного забезпечення для розгортання на активах із вищим пріоритетом включає розгляд практик безпечної розробки програмного забезпечення постачальника.				
313	ARCHITECTURE-4c	2	Захищені конфігурації програмного забезпечення необхідні як частина процесу розгортання програмного забезпечення як для придбаного програмного забезпечення, так і для програмного забезпечення, розробленого власними силами.				
314	ARCHITECTURE-4d	3	Усе програмне забезпечення, розроблене власними силами, розробляється з використанням безпечних методів розробки програмного забезпечення.				
315	ARCHITECTURE-4e	3	Вибір усього закупленого програмного забезпечення включає розгляд практик безпечної розробки програмного забезпечення постачальника.				
316	ARCHITECTURE-4f	3	Процес перегляду архітектури оцінює безпеку нових програм і аналізує програми перед їх розгортанням.				
317	ARCHITECTURE-4g	3	Автентичність усього програмного забезпечення та мікропрограм прошивки перевіряється перед розгортанням.				
318	ARCHITECTURE-4h	3	Тестування безпеки (наприклад, статичне тестування, динамічне тестування, фазинг-тестування, тестування на проникнення) виконується для власно розроблених і власно				

1	2	3	4	5	6	7	8
			спеціально розроблених програм періодично та відповідно до визначених тригерів, таких як системні зміни та зовнішні події.				
Ціль 5. Впровадити захист даних як елемент архітектури кібербезпеки							
319	ARCHITECTURE-5a	1	Конфіденційні дані захищені в стані спокою, принаймні тимчасово.				
320	ARCHITECTURE-5b	2	Усі дані, що перебувають у стані спокою, захищено для вибраних категорій даних.				
321	ARCHITECTURE-5c	2	Усі дані, що передаються, захищено для вибраних категорій даних.				
322	ARCHITECTURE-5d	2	Для вибраних категорій даних реалізовано засоби криптографічного захисту для даних у стані спокою та даних, що передаються.				
323	ARCHITECTURE-5e	2	Інфраструктура керування ключами (тобто генерація ключів, зберігання ключів, знищення ключів, оновлення ключів і відкликання ключів) реалізована для підтримки криптографічного контролю.				
324	ARCHITECTURE-5f	2	Реалізовано елементи керування для унеможливлення викрадання даних (наприклад, засоби запобігання втраті даних).				
325	ARCHITECTURE-5g	3	Архітектура кібербезпеки включає засоби захисту (наприклад, повне шифрування диска) для даних, які зберігаються на активах, які можуть бути втрачені або викрадені.				
326	ARCHITECTURE-5h	3	Архітектура кібербезпеки включає захист від несанкціонованих змін програмного забезпечення, мікропрограм прошивки обладнання та даних.				
Ціль 6. Управлінська діяльність у сфері ARCHITECTURE							
327	ARCHITECTURE-6a	3	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області ARCHITECTURE.				

1	2	3	4	5	6	7	8
328	ARCHITECTURE-6b	3	Необхідні ресурси (люди, фінансування та інструменти) надаються для підтримки діяльності в області ARCHITECTURE.				
329	ARCHITECTURE-6c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області ARCHITECTURE.				
330	ARCHITECTURE-6d	3	Відповідальність, підзвітність та повноваження щодо здійснення діяльності в області ARCHITECTURE покладаються на персонал.				
331	ARCHITECTURE-6e	3	Персонал, який виконує діяльність в області ARCHITECTURE, має навички та знання, необхідні для виконання покладених на них обов'язків.				
332	ARCHITECTURE-6f	3	Оцінюється та відслідковується ефективність діяльності в області ARCHITECTURE.				
Область: Управління програмою кібербезпеки (PROGRAM)							
Ціль 1. Створення стратегії програми кібербезпеки							
333	PROGRAM-1a	1	Організація має програмну стратегію кібербезпеки, яка може бути розроблена та керована спеціальним чином.				
334	PROGRAM-1b	2	Стратегія програми кібербезпеки визначає цілі та завдання діяльності організації з кібербезпеки.				
335	PROGRAM-1c	2	Стратегія та пріоритети програми кібербезпеки задокументовані та узгоджені з місією організації, стратегічними цілями та ризиками для критичної інфраструктури.				
336	PROGRAM-1d	2	Стратегія програми кібербезпеки визначає підхід організації до забезпечення програмного нагляду та управління діяльністю з кібербезпеки.				
337	PROGRAM-1e	2	Стратегія програми кібербезпеки визначає структуру та організацію програми кібербезпеки.				

1	2	3	4	5	6	7	8
338	PROGRAM-1f	2	Стратегія програми кібербезпеки визначає стандарти та вказівки, яких має дотримуватися програма.				
339	PROGRAM-1g	2	Стратегія програми кібербезпеки визначає будь-які застосовні вимоги відповідності, яким має відповідати програма (наприклад, ISO).				
340	PROGRAM-1h	3	Стратегія програми кібербезпеки оновлюється періодично та відповідно до визначених тригерів, таких як бізнес-зміни, зміни в операційному середовищі та зміни в профілі загроз (практика THREAT-2e).				
Ціль 2. Створення та підтримка програми з кібербезпеки							
341	PROGRAM-2a	1	Вище керівництво з відповідними повноваженнями надає підтримку програмі кібербезпеки, принаймні в окремих випадках.				
342	PROGRAM-2b	2	Програма кібербезпеки створена відповідно до стратегії програми кібербезпеки.				
343	PROGRAM-2c	2	Фінансова підтримка вищого керівництва програми кібербезпеки є помітною і активною.				
344	PROGRAM-2d	2	Фінансова підтримка вищого керівництва надається для розробки, підтримки та забезпечення дотримання політики кібербезпеки.				
345	PROGRAM-2e	2	Відповідальність за програму кібербезпеки покладено на посадову особу із достатніми повноваженнями.				
346	PROGRAM-2f	2	Визначено та залучено зацікавлені сторони для діяльності з управління програмою кібербезпеки.				
347	PROGRAM-2g	3	Діяльність програми кібербезпеки періодично переглядається, щоб переконатися, що вона відповідає стратегії програми кібербезпеки.				
348	PROGRAM-2h	3	Діяльність у сфері кібербезпеки перевіряється незалежно, щоб забезпечити відповідність політикам і процедурам				

1	2	3	4	5	6	7	8
			кібербезпеки, періодично та відповідно до визначених тригерів, таких як зміни процесів.				
349	PROGRAM-2i	3	Програма кібербезпеки спрямована на дотримання законодавчих і нормативних вимог і забезпечує її відповідність.				
350	PROGRAM-2j	3	Організація співпрацює із зовнішніми організаціями, щоб сприяти розробці та впровадженню стандартів кібербезпеки, інструкцій, передових практик, отриманих уроків і нових технологій.				
Ціль 3. Управлінська діяльність для області PROGRAM							
351	PROGRAM-3a	2	Задокументовані процедури встановлюються, дотримуються та підтримуються для діяльності в області PROGRAM.				
352	PROGRAM-3b	2	Надаються відповідні ресурси (люди, фінансування та інструменти) для підтримки заходів в області PROGRAM.				
353	PROGRAM-3c	3	Актуальні політики або інші організаційні директиви визначають вимоги до діяльності в області PROGRAM.				
354	PROGRAM-3d	3	Відповідальність, підзвітність та повноваження щодо виконання заходів в області PROGRAM покладаються на персонал.				
355	PROGRAM-3e	3	Персонал, який виконує діяльність в області PROGRAM, має навички та знання, необхідні для виконання покладених на них обов'язків.				
356	PROGRAM-3f	3	Оцінюється та відслідковується ефективність діяльності в області PROGRAM.				

Заступник начальника
Управління – начальник відділу
цифрової трансформації Управління
захисту критичної інфраструктури,
кібербезпеки та цифрового розвитку **Віталій БАЗАЛИЦЬКИЙ**

МІНІСТЕРСТВО ЕНЕРГЕТИКИ УКРАЇНИ
(Міненерго)
вул. Хрещатик, 30, м. Київ, 01601, тел.: (044) 531-36-93; 206-38-45
E-mail: kanc@mev.gov.ua, сайт: https://www.mev.gov.ua, ідентифікаційний код 37552996

_____ На № _____

Державна регуляторна служба України

Щодо погодження проєкту наказу

Міністерство енергетики України надсилає на розгляд проєкт наказу Міненерго «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж» (далі – проєкт наказу), розроблений відповідно до пункту 2 Плану заходів щодо реалізації Концепції впровадження «розумних мереж» в Україні до 2035 року, затвердженого розпорядженням Кабінету Міністрів України від 14.10.2022 № 908-р, з урахуванням доручення Прем'єр-міністра України Дениса ШМИГАЛЯ від 28.03.2024 № 40517/8/1-23, та просить погодити проєкт наказу **в триденний термін**.

Додатки: 1. Проєкт наказу на 51 арк.
2. Аналіз регуляторного впливу до проєкту наказу на 11 арк.
3. Повідомлення про оприлюднення проєкту наказу на 2 арк.
4. Копія наказу від 29 травня 2024 року № 203 «Про внесення змін до Плану діяльності Міністерства енергетики України з підготовки проектів регуляторних актів на 2024 рік» на 3 арк.

Міністр **Герман ГАЛУЩЕНКО**

Ірина ГОНЧАРЕНКО +380686741786

Аналіз регуляторного впливу
до проєкту наказу Міністерства енергетики України
«Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж»

І. Визначення проблеми

Проєкт наказу «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж» (далі – проєкт наказу) розроблено Міністерством енергетики України відповідно до пункту 2 Плану заходів щодо реалізації Концепції впровадження «розумних мереж» в Україні до 2035 року, затвердженого розпорядженням Кабінету Міністрів України від 14.10.2022 № 908-р, з урахуванням доручень Прем'єр-міністра України Дениса ШМИГАЛЯ від 28.03.2024 № 40517/8/1-23 та заступника Державного секретаря Кабінету Міністрів Олега ВОЙТОВИЧА від 05.04.2024 № 8260/0/2-24.

Постановою Кабінету Міністрів України від 09.10.2020 № 1109 «Деякі питання об'єктів критичної інфраструктури» Міненерго визначено уповноваженим органом державної влади, відповідальним за паливно-енергетичний сектор критичної інфраструктури.

Наказом Міненерго від 07.09.2022 № 1-ДСК (зі змінами) затверджено Перелік об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури.

Наказом Міненерго від 16.12.2022 № 5-ДСК (зі змінами) затверджено Перелік об'єктів критичної інформаційної інфраструктури паливно-енергетичного сектору критичної інфраструктури.

Відповідно до пункту 7 частини четвертої статті 5 Закону України «Про основні засади забезпечення кібербезпеки України» підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури, є суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки.

Одним з основних чинників, що створює небезпеку об'єктам критичної інфраструктури є кіберзагрози та кібератаки.

24.02.2022 російська федерація розпочала військову агресію проти держави Україна. У зв'язку з цим, відповідно до Указу Президента України від 24.02.2022 № 64/2022 в Україні введено воєнний стан, строк дії якого продовжено. російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно об'єктів критичної інфраструктури, в тому числі електричних мереж.

Розроблення проєкту наказу зумовлено необхідністю оцінки та вдосконалення програм з кібербезпеки електричних мереж та зміцнення їх експлуатаційної стійкості, покращення стану кібербезпеки електричних мереж, підвищення їх захищеності.

Під час визначення проблеми, яку передбачається розв’язати шляхом державного регулювання, встановлені основні групи, на які проблема справляє вплив:

Групи (підгрупи)	Так	Ні
Громадяни	-	+
Держава	+	-
Суб’єкти господарювання	+	-

Ця проблема не може бути вирішена за допомогою ринкових механізмів, оскільки визначення моделі зрілості спроможностей кібербезпеки електричних мереж, індикаторів та індексів стану кібербезпеки електричних мереж можливе лише за допомогою державного регулювання.

II. Цілі державного регулювання

Основною ціллю проєкту наказу є затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж, що визначає модель зрілості спроможностей кібербезпеки електричних мереж, яка базується на моделі зрілості спроможностей кібербезпеки Cybersecurity capability maturity model program (C2M2). Модель C2M2 призначена для використання операторами критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури з метою здійснення самооцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж, як об’єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури.

III. Визначення та оцінка альтернативних способів досягнення цілей

1. Визначення альтернативних способів

Вид альтернативи	Опис альтернативи
Альтернатива 1	Залишення існуючої ситуації без змін. Відсутність об’єктивної інформації щодо оцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж, як об’єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури, в цілому призведе до збільшення ризиків порушення стабільного функціонування електричних мереж внаслідок кібератак.
Альтернатива 2	Прийняття проєкту наказу. Прийняття проєкту наказу забезпечить досягнення вищезгаданих цілей державного регулювання повною мірою.

2. Оцінка обраних альтернативних способів досягнення цілей

Оцінка впливу на сферу інтересів держави

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні.	Відсутність нормативно-правової бази щодо оцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж. Збереження існуючої ситуації збільшує ризик значних матеріальних збитків внаслідок масштабних кібератак.
Альтернатива 2	Прийняття проєкту наказу забезпечить: - виконання пункту 2 Плану заходів щодо реалізації Концепції впровадження «розумних мереж» в Україні до 2035 року, затвердженого розпорядженням Кабінету Міністрів України від 14.10.2022 № 908-р, з урахуванням доручень Прем'єр-міністра України Дениса ШМИГАЛЯ від 28.03.2024 № 40517/8/1-23 та заступника Державного секретаря Кабінету Міністрів Олега ВОЙТОВИЧА від 05.04.2024 № 8260/0/2-24; - оцінку та вдосконалення програми з кібербезпеки електричних мереж; - зміцнення кіберстійкості та покращення стану кібербезпеки електричних мереж. Це дозволить об'єктивно оцінити реальний стан кібербезпеки електричних мереж з урахуванням реальних і потенційних загроз у кіберпросторі та визначити напрями	Відсутні.

	вдосконалення і розвитку системи кібербезпеки електричних мереж, що в свою чергу забезпечить можливість суттєвого зменшення імовірності виникнення аварійних ситуацій та аварій (спричинених кібератаками) з вкрай негативними наслідками для держави, населення та навколишнього природного середовища.	

Оцінка впливу на громадян не проводилась, оскільки положення проєкту наказу на них не поширюються.

Оцінка впливу на сферу інтересів суб'єктів господарювання (операторів критичної інфраструктури) *

Показник	Великі	Середні	Малі	Мікро	Разом
Кількість суб'єктів господарювання, що підпадають під дію регулювання (одиниць)	69	66	-	-	135
Питома вага групи у загальній кількості, відсотків	51,1	48,9	-	-	100

* Відповідно до Переліку об'єктів критичної інфраструктури паливно-енергетичного сектору критичної інфраструктури, затвердженого наказом Міністерства енергетики України від 07.09.2022 № 1-ДСК (зі змінами).

Вид альтернативи	Вигоди	Витрати
Альтернатива 1	Відсутні.	Негативний вплив на безпеку електричних мереж через ризик виникнення аварійних ситуацій або аварій внаслідок можливих кібератак. Виникнення аварійних ситуацій через кібератаки може призвести до значних матеріальних збитків. Виникнення аварій через

		кібератаки може призвести до забруднення навколишнього природного середовища, нанесення шкоди здоров'ю персоналу та населенню, значних витрат на ліквідацію наслідків аварії.
Альтернатива 2	Покращення стану кібербезпеки електричних мереж завдяки реалізації програм з удосконалення кібербезпеки. Зменшення імовірності виникнення аварійних ситуацій наслідок кібератак. Забезпечення стабільно безпечної та економічно ефективної роботи електричних мереж.	Відсутні.

Витрати на одного суб'єкта господарювання великого підприємництва і середнього підприємництва, які виникають внаслідок дії регуляторного акта (згідно з додатком 2 до Методики проведення аналізу впливу регуляторного акта).

Порядковий номер	Витрати	За перший рік	За п'ять років
1	Витрати на придбання основних фондів, обладнання та приладів, сервісне обслуговування, навчання/підвищення кваліфікації персоналу тощо, гривень.	0,00	0,00
2	Податки та збори (зміна розміру податків/зборів, виникнення необхідності у сплаті податків/зборів), гривень.	0,00	0,00
3	Витрати, пов'язані із веденням обліку, підготовкою та поданням звітності державним органам, гривень.	3000,00	5000,00
4	Витрати, пов'язані з адмініструванням заходів	0,00	0,00

	державного нагляду (контролю) (перевірок, штрафних санкцій, виконання рішень/ приписів тощо), гривень.		
5	Витрати на отримання адміністративних послуг (дозволів, ліцензій, сертифікатів, атестатів, погоджень, висновків, проведення незалежних/обов'язкових експертиз, сертифікації, атестації тощо) та інших послуг (проведення наукових, інших експертиз, страхування тощо), гривень.	0,00	0,00
6	Витрати на оборотні активи (матеріали, канцелярські товари тощо), гривень.	200,00	1000,00
7	Витрати, пов'язані із наймом додаткового персоналу, гривень.	0,00	0,00
8	Інше (уточнити), гривень.	0,00	0,00
9	РАЗОМ (сума рядків: 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8), гривень.	3200,00	6000,00
10	Кількість суб'єктів господарювання великого та середнього підприємництва, на яких буде поширено регулювання, одиниць.	135	135
11	Сумарні витрати суб'єктів господарювання великого та середнього підприємництва, на виконання регулювання (вартість регулювання) (рядок 9 х рядок 10), гривень.	432000,00	810000,00

Сумарні витрати за альтернативами	Сума витрат, гривень
Альтернатива 1	Надвеликі витрати на ліквідацію наслідків аварій в електричних

	мережах.
Альтернатива 2	810000,00

IV. Вибір найбільш оптимального альтернативного способу досягнення цілей

Рейтинг результативності (досягнення цілей під час вирішення проблеми)	Бал результативності (за чотирибальною системою оцінки)	Коментарі щодо присвоєння відповідного бала
Альтернатива 1	1	Цілі регулювання не можуть бути досягнуті (проблема продовжить існувати).
Альтернатива 2	4	Прийняття проєкту наказу забезпечить повною мірою досягнення поставлених цілей.

Рейтинг результативності	Вигоди (підсумок)	Витрати (підсумок)	Обґрунтування відповідного місця альтернативи у рейтингу
Альтернатива 1	Відсутні.	Відсутність нормативно-правової бази щодо оцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж призводить до відсутності об’єктивної інформації щодо оцінки рівня кібербезпеки електричних мереж, як наслідок, до вразливості об’єктів критичної інфраструктури у кіберпросторі. Збереження існуючої ситуації збільшує ризик значних	Альтернатива не забезпечує досягнення цілей регулювання. За відсутності вигод, кількість неврегульованих витрат залишається значною.

		матеріальних збитків внаслідок кібератак. Негативний вплив на безпеку електричних мереж через ризик виникнення аварійних ситуацій або аварій внаслідок можливих кібератак, спрямованих на електричні мережі.	
Альтернатива 2	Прийняття проєкту наказу забезпечить: - затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж; - визначення: моделі зрілості спроможностей кібербезпеки електричних мереж, як об'єктів критичної інфраструктури; індикаторів та індексів стану кібербезпеки електричних мереж; - проведення самооцінки стану кіберзахисту електричних мереж; - отримання об'єктивної та повної оцінки рівня кібербезпеки електричних мереж, як об'єктів критичної інфраструктури. - формування пропозицій щодо вдосконалення законодавства у	Відсутні.	Альтернатива забезпечує досягнення цілей регулювання. За відсутності витрат, дозволяє досягнути максимальної кількості вигод.

	сфері кібербезпеки, кіберзахисту та визначення напрямів розвитку системи кібербезпеки паливно-енергетичного сектору критичної інфраструктури в частині кіберзахисту; - планування заходів щодо забезпечення кіберстійкості електричних мереж. Це призведе до визначення напрямів вдосконалення і розвитку електричних мереж, що суттєво зменшить імовірність виникнення аварійних ситуацій та аварій (спричинених кібератаками) з вкрай негативними наслідками для держави, населення та навколишнього природного середовища.		

V. Механізми та заходи, які забезпечать розв’язання визначеної проблеми

Механізмами, що забезпечать розв’язання визначеної проблеми, є прийняття проєкту наказу.

Проєктом наказу пропонується: затвердити Методику оцінювання стану кібербезпеки електричних мереж; практики кібербезпеки електричних мереж.

Організаційні заходи, які необхідно здійснити Міністерству енергетики України для впровадження наказу «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж»:

- направлення операторам критичної інфраструктури інформаційних листів щодо набрання чинності регуляторним актом;

- розміщення на сайті Міністерства енергетики України www.mev.gov.ua наказу «Про затвердження Методики оцінювання стану кібербезпеки електричних мереж та практик кібербезпеки електричних мереж»;

- проведення операторами критичної інфраструктури самооцінки стану кібербезпеки та виконання заходів з кіберзахисту електричних мереж, як об'єктів критичної інфраструктури;

- підготовка звітів за результатами застосування моделі C2M2, що надсилаються операторам критичної інфраструктури до Міненерго.

VI. Оцінка виконання вимог регуляторного акта залежно від ресурсів, якими розпоряджаються органи виконавчої влади чи органи місцевого самоврядування, фізичні та юридичні особи, які повинні проваджувати або виконувати ці вимоги

Реалізація регуляторного акта не потребуватиме додаткових бюджетних витрат і ресурсів на адміністрування регулювання органами виконавчої влади чи органами місцевого самоврядування.

М-тест не проводився оскільки малі суб'єкти господарювання не зазнають витрат на впровадження регуляторного акта.

VII. Обґрунтування запропонованого строку дії регуляторного акта

Регуляторний акт набирає чинності з дня його офіційного опублікування.

Строк дії цього регуляторного акта не обмежується у часі, що надасть можливість розв'язати проблеми та досягти цілей державного регулювання.

VIII. Визначення показників результативності дії регуляторного акта

Прогнозними значеннями показників результативності регуляторного акта є:

- розмір надходжень до державного та місцевих бюджетів і державних цільових фондів, пов'язаних з дією акта – не передбачається;

- кількість суб'єктів господарювання, на яких поширюється дія акта: 135 суб'єктів господарювання (операторів критичної інфраструктури), які підпадають під дію регулювання регуляторного акта;

- розмір коштів і час, що витрачатимуться органами виконавчої влади, пов'язаними з виконанням вимог акта – не змінюється (в межах робочого часу працівників та коштів, передбачених на фінансування заробітної плати для них);

- рівень поінформованості суб'єктів господарювання з основних положень акта – середній. Проєкт акта розміщено на веб-сайті Міністерства енергетики України www.mev.gov.ua, а після прийняття акта він буде розміщений на сайті www.zakon.rada.gov.ua.

- кількість скарг/звернень громадян/суб'єктів господарювання, пов'язаних із дією регуляторного акта;

- кількість погоджених документів;

- кількість виявлених порушень, пов'язаних із дією акта.

IX. Визначення заходів, за допомогою яких здійснюватиметься відстеження результативності дії регуляторного акта

Базове відстеження результативності регуляторного акта здійснюється після набрання чинності цим регуляторним актом, але не пізніше дня, з якого починається проведення повторного відстеження результативності цього акта.

Повторне відстеження результативності регуляторного акта здійснюється через 1 рік з дня набрання ним чинності.

Періодичні відстеження результативності регуляторного акта здійснюються раз на кожні три роки починаючи з дня закінчення заходів з повторного відстеження результативності цього акта.

Міністр енергетики України **Герман ГАЛУЩЕНКО**

«___» _____ 2024 року