ОЦІНКА НАЦІОНАЛЬНИХ КІБЕРСПРОМОЖНОСТЕЙ:

ЯКИМ Є РІВЕНЬ КІБЕРЗРІЛОСТІ УКРАЇНИ ВІДПОВІДНО ДО МЕТОДОЛОГІЇ ENISA?

Дослідження «Оцінка національних кіберспроможностей: яким є рівень кіберзрілості України відповідно до методології ENISA?» підготовлене Інститутом дослідження кібервійни завдяки підтримці, наданій Агентством США з міжнародного розвитку (USAID), через Проєкт USAID «Кібербезпека критично важливої інфраструктури України». Думки авторів, висловлені в цьому дослідженні, не обов'язково відображають погляди Агентства США з міжнародного розвитку або Уряду США

ЗМІСТ

ВСТУП

Кіберкомпонента продовжує залишатись важливим елементом російських гібридних зусиль, які доповнюють військові заходи проти України.

Україна зі свого боку, зокрема– за значної допомоги міжнародних партнерів, активно здійснює реформи власної системи кібербезпеки, нарощує технічні та кадрові спроможності, обмінюється інформацією з партнерами та імплементує міжнародні стандарти й підходи.

Останнє особливо важливо з огляду на чіткий євроінтеграційний курс України, а отже, і необхідність зближення підходів з європейськими партнерами – у принципах формування державної політики, пріоритетах такої політики та розвитку технічних спроможностей.

13 листопада 2023 року Україна та Агентство Європейського Союзу з кібербезпеки (ENISA) уклали Робочу угоду, мета якої – підвищити обізнаність сторін для посилення кіберстійкості, обміну найкращими практиками для забезпечення гармонізації законодавства та імплементації, а також обмін знаннями та інформацією щодо ландшафту загроз кібербезпеці.

ENISA є ключовим органом ЄС, який надає всім країнам методологічну допомогу в питаннях розвитку кібербезпеки, сприяє процесу обміну інформацією та найкращими практиками, а також формує спільний для всіх європейських країн простір настанов з кібербезпеки, що мають зробити країни більш стійкими до кіберзагроз.

Україна має стати частиною європейського кібербезпекового простору, бути частиною європейської кіберсім'ї. А це не можливо без тісної взаємодії з європейськими інституціями, спільного розуміння ландшафту кіберзагроз та кіберпотенціалів європейських країн. Однак без кількісного вимірювання цього потенціалу, чіткого розуміння рівня впровадженості кібербезпекових практик складно зрозуміти траєкторію руху до ліпшої кіберстійкості.

У 2020 році ENISA спробувала вирішити це завдання, запропонувавши всім країнам власну методологію вимірювання рівня кіберзрілості – «National Capabilities Assessment Framework». Документ дає конкретні рекомендації та настанови країнам для оцінки того, наскільки вдало вони впровадили найкращі практики та ключові політики на шляху розвитку кібербезпеки. Це дослідження має на меті започаткувати процес оцінки національного рівня кіберзрілості України, аби сприяти становленню нашої країни частиною загального простору кібербезпеки ЄС.

Це перша спроба, яка має не лише дати відповідні результати, що базуються на підходах ENISA, але й допомогти зрозуміти межі застосування цієї моделі оцінки, запропонувати можливі уточнення застосування методології та порядку проведення оцінки в майбутньому.

Оцінка рівня кіберзрілості – це не лише важливий елемент оцінки поточного стану національної кібербезпеки, але й набір цінних даних напередодні оновлення ключового стратегічного документу – Стратегії кібербезпеки України. Це можливість критично поглянути на поточні досягнення й зрозуміти, які ідеї та завдання потребують включення в оновлений стратегічний документ.

Таке визначення рівня кіберзрілості – це також можливість додатково оцінити ефективність поступового виконання Стратегії в довгостроковій перспективі.

МЕТОДОЛОГІЯ ТА ДИЗАЙН ДОСЛІДЖЕННЯ

В основі цього дослідження – адаптований варіант методології ENISA "Настанови з оцінки національних спроможностей"[1] (National Capabilities Assessment Framework), що містить ключові підходи до проведення комплексної оцінки країн ЄС щодо їхньої кіберзрілості.

Така оцінка проводиться за двома основними напрямками: оцінка зрілості стратегічного підходу до сфери кібербезпеки (фактично – наявності стратегічних документів та певних національних політик / практик) та оцінка зрілості кібер-спроможності, що має на меті визначити реальний кіберпотенціал країни в 17 різних сферах (цілях). До таких цілей належать:

- ✓ розробка Національного плану (планів) реагування на інциденти кібербезпеки;
- ✓ встановлення базових заходів безпеки;
- ✓ забезпечення захисту цифрової ідентифікації та зміцнення довіри до цифрових державних послуг;
- ✓ встановлення спроможностей реагування на інциденти;
- ✓ підвищення обізнаності користувачів;
- ✓ організація тренувань з кібербезпеки;
- ✓ посилення навчальних та освітніх програм;
- ✓ сприяння науково-дослідним і дослідно-конструкторським роботам;
- ✓ забезпечення стимулів для приватного сектору інвестувати в заходи безпеки;
- ✓ покращення кібербезпеки ланцюга постачання;
- ✓ захист критичної інформаційної інфраструктури (КІІ), операторів основних послуг і провайдерів цифрових послуг;
- ✓ протидія кіберзлочинності;
- ✓ встановлення механізмів звітування про інциденти;
- ✓ посилення захисту конфіденційності даних;
- ✓ встановлення державно-приватного партнерства (ДПП);
- ✓ надання інституційного характеру співпраці між державними органами;
- ✓ долучення до міжнародної співпраці (не тільки з країнами-членами ЄАС).

Оцінка зрілості стратегічного підходу до сфери кібербезпеки визначається через набір ідентичних, повторюваних питань для кожного блоку (питання блоків a, b та c).

Для оцінки зрілості кіберспроможності використовуються питання блоків від 1 до 13 (різна кількість питань в різних цілях для визначення рівня зрілості). Загалом цей блок містить 319 питань.

Обидва блоки містять «обов'язкові» (позначені «1» у стовпчику R) та «вторинні» (не критичні для підтвердження рівня кіберзрілості

[1] https://www.enisa.europa.eu/publications/national-capabilities-assessment-framework

позначені «0» у стовпчику R) питання. Усі питання мають варіант відповіді лише «Так» або «Ні».

Загальна вимога до визначення будь-якого з вище описаних рівнів зрілості – послідовність. За такого підходу для переходу до наступного рівня кіберзрілості потрібне повне виконання вимог певного рівня зрілості (позитивні відповіді на всі «обов'язкові» питання). Відповідно не можливо перейти до наступного рівня, якщо всі задачі попереднього не були виконані.

Також методологія ENISA пропонує додатково визначати масштаб покриття національних зусиль для кожної цілі – фактично мова йде про оцінку загальних зусиль країни в межах певної цілі, за якого ці зусилля можуть бути більш вагомими, ніж формальне визначення рівня кіберзрілості.

Хоча базова методологія передбачає можливість зміни кількості цілей для оцінки, а також певну корекцію методології (для більшої налаштованості під ситуацію кожної конкретної країни), однак для цього дослідження було обрано підхід максимально повного слідування базовим настановам з метою формування показника, який максимально наближений за логікою формування до методологічних припущень ENISA.

Польова частина дослідження проводилась у період з лютого по березень 2024 року і містила в собі формування опитувальників відповідно до настанов ENISA, їх надсилання респондентам, а також опрацювання отриманих результатів. Також у період з квітня по травень 2024 року експерти опрацьовували окремі показники опитувальника та внесли деякі корективи в підсумкові відповіді (як, наприклад, у базових опитувальниках не був відображений факт створення Міжвідомчої робочої групи з питань залучення міжнародної допомоги для забезпечення кібербезпеки та кіберстійкості держави).

Усього в межах дослідження було опитано 40 організацій, що містять в собі всіх членів НКЦК, 10 ЦОВВ, 20 обласних державних адміністрацій, 2 наукові установи та 1 приватну компанію, що надає послуги в сфері кібербезпеки.

ЗАГАЛЬНІ ВИСНОВКИ ДОСЛІДЖЕННЯ

☑ Чинна нормативна база (передусім – Стратегія кібербезпеки України та щорічні плани її виконання) **майже відповідає третьому рівню** зрілості стратегічного підходу до сфери кібербезпеки.

☑ Особливо помітними є здобутки (5 рівень зрілості стратегічного підходу) для:

національних планів реагування на інциденти кібербезпеки;

науково-дослідних і дослідно-конструкторських робіт;

захисту критичної інформаційної інфраструктури;

протидії кіберзлочинності.

☑ Респонденти також визначили як 5 рівень зрілості стратегічний підхід до розвитку державно-приватного партнерства в Україні. Водночас як підтверджувальні показники наводяться лише завдання Стратегії кібербезпеки України та щорічного плану її реалізації. У майбутніх оцінках це питання підлягатиме більш виваженій оцінці з метою уточнення ключових здобутків у цій сфері.

☑ Стратегічно найскладніша ситуація у 3 сферах (у кожній з цих сфер рівень зрілості політик не перевищує одиницю):

забезпечення стимулів для приватного сектору інвестувати в заходи безпеки;

кібербезпека ланцюгів постачання;

захист конфіденційності даних.

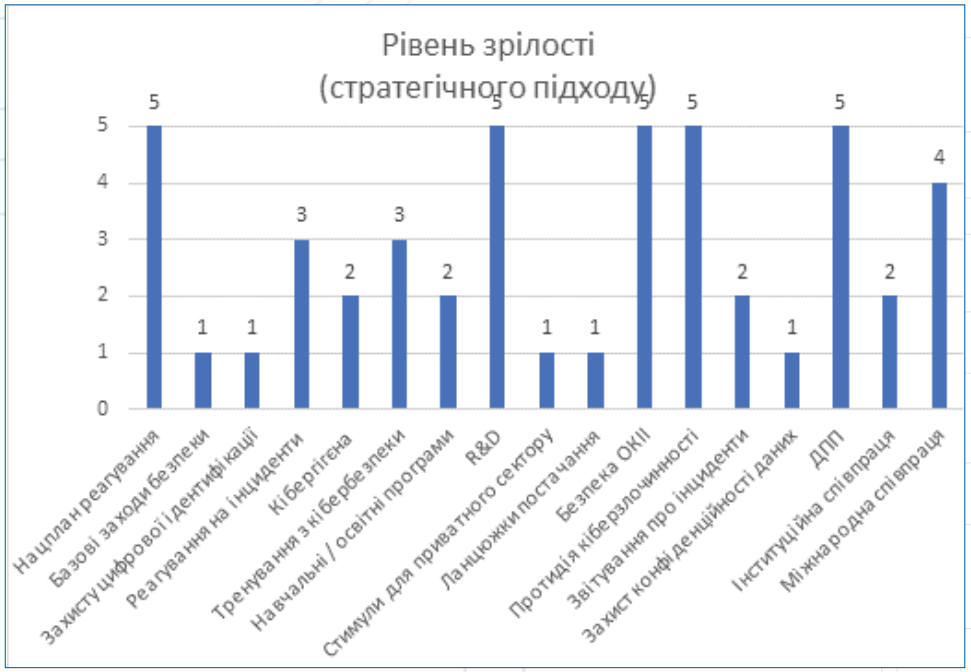
☑ Безпека ланцюгів постачання найменш реалізована з цілей. Тут не лише рівень зрілості стратегічного підходу дорівнює одиниці, але Україна не змогла набрати навіть першого рівня кіберзрілості в частині кіберспроможностей: не виконано навіть першої базової задачі.

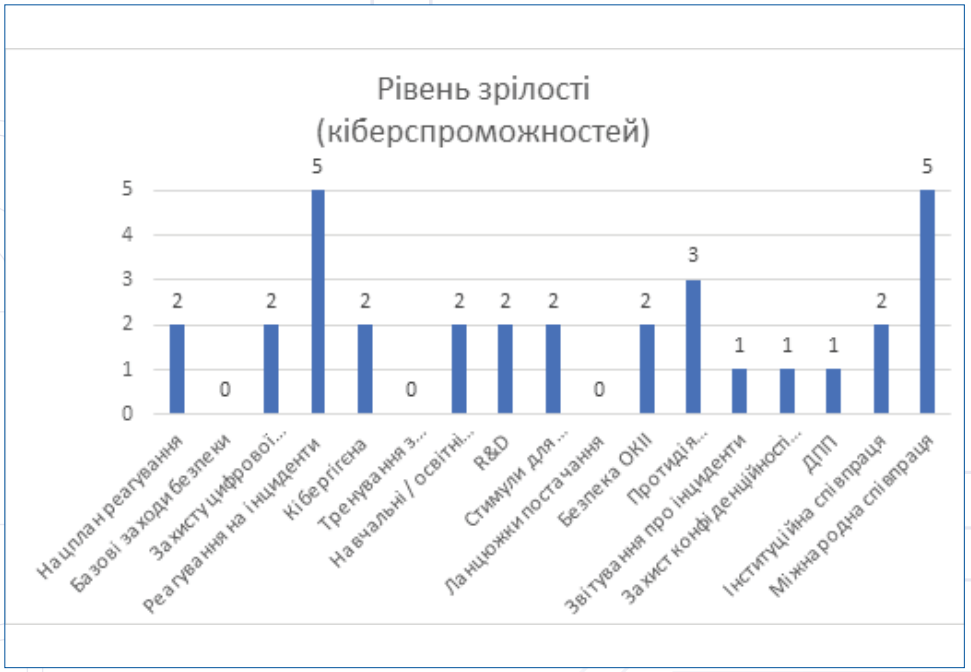
☑ Хоча **виявлений середній рівень зрілості кіберспроможностей** майже **відповідає 2 рівню зрілості**, однак цей показник не повною мірою відповідає реальним зусиллям уряду. За останній відповідає показник «масштаб покриття» – відсоток позитивних відповідей на питання таблиці відносно загальної кількості питань. Показовими в цьому сенсі є три групи показників:

встановлення базових заходів безпеки. За формальною ознакою рівень зрілості кіберспроможностей тут нульовий: не виконано дві базові задачі. Однак масштаб покриття для цієї цілі – 74%. Держава виконала переважну кількість задач, які відповідають 4 і навіть 5 рівню кіберзрілості;

організація тренувань з кібербезпеки. Через нереалізованість однієї з двох задач першого рівня зрілості Україні не вдалось дістатися тут навіть першого рівня кіберзрілості. Однак масштаб покриття тут – 68% (виконано більшість задач для 3 та 4 рівнів кіберзрілості);

інституційний характер співпраці між державними органами. За цим показником рівень зрілості кіберспроможностей – 2. Однак масштаб покриття – 90%. Респонденти негативно оцінили лише 1 пункт із задач цієї цілі, який є обов'язковим для отримання 3 рівня зрілості.





☑ Загалом найбільша кількість негативних відповідей була стосовно відсутності (для різних цілей) інструментів оцінки ефективності заходів, що впроваджуються, а відтак – їхнього корегування. Фактично український підхід щодо планування передбачає здебільшого цілевказання, але не дає гнучкості в корегуванні підходу чи оцінці його ефективності.

☑ Деякі позиції є не зовсім релевантними українським умовам (що знижувало бал відповідей), однак є важливими з погляду розуміння пріоритетів розвитку. Наприклад, одразу в декількох стратегічних цілях одним з показників є формалізована взаємодія з загальноєвропейськими інституціями. Україна, яка не є членом ЄС, не може виконати вказані вимоги. Однак ці пункти вказують на

№	Рівень зрілості (стратегічного підходу)	Рівень зрілості (кіберспроможностей)	Масштаб покриття (у відсотках)	Назва Цілі
1	5	2	87%	розробка Національного плану (планів) реагування на інциденти кібербезпеки
2	1	0	74%	встановлення базових заходів безпеки
3	1	2	88%	забезпечення захисту цифрової ідентифікації та зміцнення довіри до цифрових державних послуг
4	3	5	100%	встановлення спроможностей реагування на інциденти
5	2	2	53%	підвищення обізнаності користувачів
6	3	0	68%	організація тренувань з кібербезпеки
7	2	2	76%	посилення навчальних та освітніх програм
8	5	2	83%	сприяння науково-дослідним і дослідно-конструкторським роботам
9	1	2	36%	забезпечення стимулів для приватного сектору інвестувати в заходи безпеки
10	1	0	13%	покращення кібербезпеки ланцюга постачання
11	5	2	67%	захист критичної інформаційної інфраструктури (КІІ), операторів основних послуг і провайдерів цифрових послуг
12	5	3	95%	протидія кіберзлочинності
13	2	1	67%	встановлення механізмів звітування про інциденти
14	1	1	25%	посилення захисту конфіденційності даних
15	5	1	56%	встановлення державно-приватного партнерства (ДПП)
16	2	2	90%	надання інституційного характеру співпраці між державними органами
17	4	5	100%	долучення до міжнародної співпраці (не тільки з країнами-членами ЄС)

ті європейські формати, до яких Україна має долучитись вже найближчим часом.

☑ Україна має низку здобутків та чинних програм з кібер-грамотності. Водночас, як показує аналіз питань та відповідей щодо Цілі 5, українській політиці не вистачає інституційності та системності в цьому питанні. Точкові заходи чи створення контенту, що не вбудований у більш загальну стратегію підвищення цифрової обізнаності, відсутність заходів із перегляду цієї комунікаційної діяльності – усе це зменшило позиції України щодо рівня зрілості за цим пунктом.

☑ Схожа ситуація з Ціллю 6 – тренування з кібербезпеки. Останніми роками такі тренування проводяться все частіше, однак фактором, що зменшив тут показники України, стала відсутність системності в цьому процесі, а також усталеної та зрозумілої практики «вивчення уроків» (імплементації нових напрацювань після тренінгів чи аналізу кризових ситуацій).

☑ Істотні проблеми спостерігаються щодо Цілі 9 – стимули для приватного сектору. Для ЄС є традиційним підхід, коли приватний сектор активно включений в кібербезпекову діяльність завдяки зрозумілій системі стимулів та компенсацій (аналогічний підхід закладено в Акті про кіберсолдіарність ЄС). Водночас цей підхід спирається на наявні загальноєвропейські ресурси, відповідну напрацьовану практику і здебільшого мирний поступальний розвиток ЄС. В умовах війни, жорсткої нестачі фінансових та людських ресурсів можливості України в стимулюванні приватного сектору в цих питаннях досить обмежені. Можливо, у поточному вигляді ця Ціль не може бути повністю застосована до України (принаймні на цьому етапі) або має бути трансформована з урахуванням об'єктивної військово-політичної ситуації в країні.

☑ Уже згадана на початку висновків проблема з безпекою ланцюжків постачання (Ціль 10). У цьому питанні відсутня як цілісна державна політика, так і практичні кроки на рівні регламентів, правил та методичних матеріалів. Це те питання, де Україні будуть потрібні найбільші зусилля, особливо зважаючи на зростання загроз великим ОКІ через атаки такого типу.

☑ Хоча загалом успіхи України в реалізації Цілі 11 (безпека ОКІ) досить вдалі, але респонденти вказують на проблему картографування загроз ОКІ, відсутність національного реєстру ризиків, брак розуміння взаємозалежностей ОКІ (як на національному, так і міжнародному рівнях). Водночас ці напрямки діяльності зрозумілі та можуть бути достатньо швидко виправлені.

☑ Захист персональних даних (Ціль 14) – також один із важливих майбутніх фокусів для підвищення рівня кіберзрілості. Незважаючи на розвинуте законодавство в частині захисту персональних даних, кібербезпековий аспект цього захисту, звітування про кіберінциденти, у результаті яких відбулись витоки персональних даних, поширення серед різних цільових груп інформації про найкращі практики захисту персональних даних, усе це ще потребує особливої уваги з боку держави.

☑ Державно-приватне партнерство (Ціль 15) хоча і є елементом постійних дискусій в експертному співтоваристві, однак з інституалізацією та визначенням конкретних форм такої співпраці

в Україні все ще складно. Лише перший рівень кіберзрілості в частині спроможностей вказує на те, що багато важливих елементів досі не впроваджено: відсутній орган, який координує питання державно-приватного партнерства в кіберсфері, відсутній національний план щодо розвитку цього напряму, не передбачені в бюджетах організацій фінансування такої співпраці тощо.

☑ Позитивною є ситуація зі співпрацею між державними суб'єктами (Ціль 16). Єдиною помітною проблемою залишається брак взаємодії та співпраці кіберфахівців на регіональному рівні:для них немає постійних (чи хоча б регулярних) форматів взаємодії, де вони могли б обмінятися досвідом та найкращими практиками.

☑ Міжнародна співпраця (Ціль 17), напевно, найбільш динамічна та повна на сьогодні. Єдиним застереженням експертів була відсутність механізму, що забезпечує динамічну адаптацію плану дій щодо цієї Цілі відповідно до змін середовища. Хоча експерти констатували відсутність такого механізму, водночас не можна не зауважити, що таким механізмом може бути формат двосторонніх та багатосторонніх діалогів, порядок денний до яких формується якраз відповідно до поточних потреб України. Ще одним таким механізмом може стати Талліннський механізм.

ОРГАНІЗАЦІЙНІ ВИСНОВКИ

Хоча основною метою дослідження було визначити рівень кіберзрілості України, однак сам процес анкетування, збору результатів та аналіз ходу дослідження дозволяє зробити низку висновків щодо самого цього процесу й стати у пригоді під час проведення майбутніх досліджень за цією методологією. До таких висновків можна віднести:

☑ Помітними є відмінності в якості заповнення анкет. Основні суб'єкти національної системи кібербезпеки здебільшого відповідально підійшли до заповнення (додаючи там, де це можливо, підтверджувальні коментарі чи посилання), органи місцевого самоврядування, наукові організації та не профільні ЦОВВ заповнювали анкети або частково (багато полів залишилися взагалі незаповненими), або не надавали підтверджувальних позицій.

☑ Для майбутніх етапів проведення такої оцінки очевидною є необхідність додавання ще одного поля до кожного питання з коротким поясненням його сутності. Помітно, що в багатьох випадках респонденти відповідали на питання з позиції ситуації у їхній організації, а не в загальнонаціональному контексті. Особливо складною була ситуація з питаннями блоку оцінки стратегічного підходу. Базова методологія передбачала широке коло питань, які дозволяли гнучко описати реальні здобутки країни на цьому шляху. Однак для високонормативної української практики цей підхід не дуже вдалий.

☑ Відсутність підтверджувальних позицій у багатьох питаннях сильно ускладнює аналіз реальних здобутків. За повної відсутності підтверджувальних позицій для деяких питань автори цього дослідження виходили з позиції переважання простої більшості відповідей на певне питання («Так» чи «Ні»), що з погляду оцінки реального результату є певним припущенням.

☑ Виключно анонімне опитування має недостатньо ефективний вигляд для такого дослідження. Базова гіпотеза дослідження передбачала, що опитування достатньої кількості залучених у проблематику експертів з можливістю надати їм необхідні коментарі до своїх відповідей (за жорсткої моделі основної відповіді у дихотомії «Так» чи «Ні») дозволить зібрати належний емпіричний матеріал. Велика кількість відповідей без підтвердження вказує на необхідність доповнення анкетування методом опитування (глибинних інтерв'ю) або стратегічних сесій із представниками членів НКЦК для формування первинних оцінок, відсилок на підтверджувальні документи або можливості зафіксувати оцінки респондентів, які не можуть бути підтверджені відповідними документами чи посиланнями.

☑ Методологія потребує доопрацювання та доналаштування. Хоча дослідження спирається на максимально наближене до базових питань ENISA (з незначними корегуваннями відповідно до національних особливостей), однак деякі з питань, які наявні в опитувальнику, не релевантні поточній ситуації. Наприклад, про ступінь впровадженості NIS Директиви. Україна не мала таких зобов'язань у минулому, однак наразі готується до впровадження NIS2 Директиви. Такі питання потребують істотного оновлення.

ДОДАТКИ

Ціль 1 - розробити Національні плани реагування на інциденти кібербезпеки

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b		1	Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?			
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?							
1	Чи розпочато роботу над розробкою національних планів реагування на		Чи існує доктрина / національна стратегія, яка включає кібербезпеку як фактор		Чи існує план управління кіберкризами на національному рівні?		Чи задоволені ви кількістю або відсотком критично важливих секторів, включених до національного плану		Чи існує процес вивчення надбаного досвіду після тренувань з кібербезпеки або реальних криз на	

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
1	інциденти кібербезпеки? Наприклад, викладення загальних цілей, сфери застосування та/або принципів планів реагування на інциденти тощо.		кризової ситуації (тобто проєкт, політика тощо)?				реагування на інциденти кібербезпеки?		національному рівні?	
2	Чи загальновідомо, що кіберінциденти є фактором кризової ситуації, який може загрожувати національній безпеці?	0	Чи існує центр для отримання інформації та інформування осіб, що ухвалюють рішення? Тобто будь-які методи, платформи або місця, аби забезпечити всім учасникам реагування на кризову ситуацію, можливість доступу до тієї ж самої інформації про кіберкризу в реальному часі.	1	Чи існують процедури на національному рівні, спрямовані на вирішення кіберкриз?	1	Чи достатньо часто організовуються заходи (тобто тренування), пов'язані з національним плануванням реагування на інциденти кібербезпеки?	1	Чи існує процес регулярного тестування національного плану?	1
3	Чи проводилися дослідження (технічні, операційні, організаційно-управлінські) в галузі планування реагування на інциденти кібербезпеки?	0	Чи залучені відповідні ресурси для нагляду за розробкою та виконанням національних планів реагування на інциденти кібербезпеки?	1	Чи існує у вашій організації комунікаційна команда, спеціально підготовлена для реагування на кіберкризи та інформування громадськості?	1	Чи достатньо у вашій організації людей, що займаються плануванням кризових ситуацій, вивченням надбаного досвіду та впровадженням змін?	1	Чи створені адекватні інструменти та платформи для формування ситуативної обізнаності?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
4			Чи існує на національному рівні методологія оцінки кіберзагрози, яка включає процедури оцінки впливу?	0	Чи залучаються всі відповідні національні зацікавлені особи (органи сектору безпеки та оборони, цивільного захисту, правоохоронні органи, міністерства, органів влади тощо)?	1	Чи достатньо у вас в організації людей, підготовлених реагувати на кіберкризи на національному рівні?	1	Чи дотримуєтесь ви конкретної моделі зрілості для моніторингу та вдосконалення плану реагування на інциденти кібербезпеки?	0
5					Чи є у вас адекватні засоби управління кризовими ситуаціями та ситуаційні кімнати?	1		1	Чи є у вас ресурси, які спеціалізуються або на передбаченні загрози, або працюють над перспективною кібербезпекою для вирішення майбутніх криз або завтрашніх викликів?	0
6					Чи взаємодієте ви з міжнародними зацікавленими суб'єкти в ЄС у разі потреби?	0				
7					Чи взаємодієте ви з міжнародними зацікавленими суб'єктами з країн, які не є членами ЄС, у разі потреби?	0				

Рекомендації

- ✓ мають бути завершені роботи з підготовки та затвердження Національного плану реагування на кіберінциденти (необхідна умова переходу на 3 рівень зрілості);
- ✓ вказаний план має бути підданий регулярним тестуванням під час національних командно-штабних навчань (умова досягнення 5 рівня зрілості);
- ✓ також бажано опрацювати спільно з партнерами з ENISA можливе формування рівнів зрілості для такого плану.

Ціль 2 - встановити базові заходи безпеки

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності у плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи проводилися дослідження з метою визначення вимог і прогалин для громадських організацій на основі міжнародно визнаних стандартів? Наприклад, ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS тощо.	1	Чи вживаються (на рівні країни) заходи безпеки відповідно до міжнародних/національних стандартів?	1	Чи є базові заходи безпеки обов'язковими?	1	Чи існує процес періодичного оновлення базових заходів безпеки?	1	Чи існує механізми для підвищення захисту ІТС, коли не вдається відреагувати й розв'язати інциденти за допомогою базових заходів безпеки?	1
2	Чи проводились дослідження з метою визначення вимог і прогалин для приватних організацій на основі міжнародно визнаних стандартів? Наприклад, ISO27001, ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, ISA, IEC, CIS тощо.	1	Чи проводиться консультація з приватним сектором та іншими зацікавленими особами під час визначення базових заходів безпеки?	1	Чи застосовуються горизонтальні заходи безпеки в критично важливих секторах?	1	Чи впроваджений механізм моніторингу для вивчення застосування базових заходів безпеки?	1	Чи проводиться оцінка на відповідність нових стандартів, які розробляються у відповідь на останні зміни в середовищі загроз?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
3					Чи застосовуються галузеві заходи безпеки в критично важливих секторах?	1	Чи існує національний орган, який перевіряє виконання базових заходів безпеки?	1	Чи маєте або чи сприяєте ви реалізації національного процесу координованого розкриття інформації про вразливість (CVD)?	1
4					Чи відповідають базові заходи безпеки застосованим схемам сертифікації?	1	Чи запроваджено процес виявлення протягом певного проміжку часу організацій, які не дотримуються вимог?	1		
5					Чи запроваджено процес самооцінки ризиків для базових заходів безпеки?	1	Чи існує процес аудиту для забезпечення належного застосування заходів безпеки?	1		
6					Чи аналізуються обов'язкові базові заходи безпеки в процесі закупівель державними органами?	0	Чи ухвалюються стандарти безпеки для розробки критично важливих програмного та апаратного забезпечень (медичне обладнання, підключені до мережі та автономні транспортні засоби, засоби радіозв'язку, обладнання важкої промисловості тощо)?	0		

Рекомендації

✓ визначення базових вимог кібербезпеки залишається важливим елементом у досягненні високого рівня кіберзрілості (досягнення 1 рівня);

✓ рішенням НКЦК доцільно ініціювати проведення експертного дослідження з метою визначення основних вимог і прогалин кібербезпеки, що характерні для громадських організацій та приватного сектору (наприклад, на основі міжнародно визнаних стандартів, як-от: ISO27001, ISO27002, BS 15000, PCI-DSS, CobiT, NIST, IEC, CIS тощо (цей захід є необхідною умовою для досягнення 1 рівня кіберзрілості);

✓ на базі НКЦК утворити робочу групу з представників основних суб'єктів національної системи кібербезпеки, а також зацікавлених стейкхолдерів щодо розробки підходів до визначення базових вимог кібербезпеки (досягнення 2 рівня);

✓ опрацювати питання можливості встановити необхідність дотримання базових вимог кібербезпеки всіма учасниками процесу закупівель, що надають свої послуги державному сектору. Щорічно проводити оцінку ситуації із дотриманням цих вимог, зокрема через обов'язковий механізми самооцінки таких постачальників (додаткова умова досягнення 3 рівня);

✓ проводити вибіркові перевірки таких організацій на предмет реального дотримання ними базових вимог кібербезпеки;

✓ проводити щорічну оцінку відповідності нових стандартів кібербезпеки (вироблених протягом останнього календарного року) актуальному ландшафту кіберзагроз України (загальна оцінка того, чи допоможе впровадження кожного з нових стандартів реагувати на конкретну загрозу з ландшафту загроз) – (досягнення 5 рівня).

Ціль 3 - забезпечити захист цифрової ідентифікації та зміцнення довіри до цифрових державних послуг

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи проводилися дослідження або аналіз прогалин з метою визначення потреб у забезпеченні захисту цифрових державних послуг для громадян і бізнесу?	1	Чи проводиться аналіз ризиків для визначення профілю ризиків для активів або сервісів, перш ніж переносити їх у хмару або залучати будь-які проєкти цифрової трансформації?	1	Чи існує сприяння процесу впровадження методологій із вбудованим алгоритмом конфіденційності в усіх проєктах електронного урядування?	1	Чи збираються показники щодо інцидентів у сфері кібербезпеки, пов'язаних із порушенням цифрових державних послуг?	1	Чи бере Україна (або ваша організація) участь у міжнародних робочих групах для підтримання стандартів та/або розробки нових вимог до електронних довірчих послуг (електронні підписи, електронні печатки, реєстрована електронна доставка, присвоєння мітки часу, автентифікація вебсайту)? Наприклад, ETSI/CEN/CENELEC, ISO, IETF, NIST, ITU тощо.	1
2			Чи існує стратегія побудови або сприяння впровадженню безпечних національних схем електронної	1	Чи залучаються приватні зацікавлені особи до процесу розробки та надання безпечних цифрових державних	1	Чи впроваджувалося взаємне визнання засобів електронної ідентифікації з країнами-членами ЄС?	1	Чи бере Україна (або ваша організація) участь у підготовці експертних оглядів щодо схем електронної	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
2		1	ідентифікації (eID) для громадян і бізнесу?	1	послуг?	1		1	ідентифікації (eID)?	1
3			Чи існує стратегія побудови або сприяння впровадженню безпечних національних електронних довірчих послуг (електронні підписи, електронні печатки, реєстрована електронна доставка, присвоєння мітки часу, автентифікація вебсайту) для громадян і бізнесу?	1	Чи впроваджується мінімальний базовий рівень безпеки для всіх цифрових державних послуг?	1				
4			Чи існує стратегія щодо хмар електронного урядування (стратегія хмарних технологій, спрямована на уряд та державні органи,як-от міністерства, урядові установи та державні адміністративні органи тощо), яка враховує наслідки для безпеки?	0	Чи доступні будь-які схеми електронної ідентифікації для громадян і бізнесу зі значним або високим рівнем безпеки, як визначено в Додатку до Регламенту eIDAS (ЄС) № 910/2014?	1				
5					Чи існують цифрові державні послуги, що вимагають схем електронної ідентифікації зі значним або високим рівнем	1				

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
5					безпеки, як визначено в Додатку до Регламенту eIDAS (ЄС) № 910/2014?					
6					Чи існують постачальники довірчих послуг для громадян і бізнесу (електронні підписи, електронні печатки, реєстрована електронна доставка, присвоєння мітки часу, автентифікація вебсайту)?	1				
7					Чи існують постачальники довірчих послуг для громадян і бізнесу (електронні підписи, електронні печатки, реєстрована електронна доставка, присвоєння мітки часу, автентифікація вебсайту)?	0				

Рекомендації

✓ утворити постійно чинну робочу групу для формування пропозицій щодо поліпшення стану захисту цифрової ідентифікації та зміцнення довіри до цифрових державних послуг (рівень 2);

✓ визначити на рівні постанови / розпорядження Кабінету Міністрів України необхідність впровадження підходів із вбудованим алгоритмом конфіденційності у всіх проєктах електронного врядування / цифрової трансформації (рівень 4);

✓ Міністерству цифрової трансформації України розглянути можливість розпочати діалог з європейськими партнерами стосовно залучення України до проведення експертних оглядів щодо схем електронної ідентифікації (eID) (рівень 5).

Ціль 4 - встановити спроможність реагування на інциденти

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	1						
1	Чи існують неформальні спроможності реагування на інциденти, якими управляє державний або приватний сектори, або спільне керування між ними?	1	Чи існує хоча б одна офіційна національна команда CSIRT?	1	Чи існують спроможності реагування на інциденти для секторів, зазначених у Додатку II до Директиви NIS?	1	Чи визначено / запроваджено стандартизовані практики для процедур реагування на інциденти та схем класифікації інцидентів?	1	Чи існує механізми раннього виявлення, ідентифікації, запобігання, реагування та пом'якшення наслідків щодо вразливостей нульового дня?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
2			Чи мають національні команди CSIRT чітко визначений обсяг втручання? Наприклад, залежно від цільового сектору, типів інцидентів, наслідків.	1	Чи існує в Україні механізм співпраці команди CSIRT для реагування на інциденти?	1	Чи оцінюється спроможність реагувати на інциденти, аби переконатися, що у вас достатньо ресурсів та навичок для виконання завдань, викладених у пункті (2) Додатку I Директиви NIS?	1		
3			Чи мають національні команди CSIRT чітко визначений регламент стосунків з іншими національними зацікавленими особами щодо національного середовища кібербезпеки та практики реагування на інциденти (наприклад, з правоохоронними органами, військовими, інтернет-провайдерами, національним центром кібербезпеки)?	0	Чи мають національні команди CSIRT спроможність реагувати на інцидент відповідно до Додатка I Директиви NIS? Тобто доступність, фізична безпека, безперервність роботи бізнесу, міжнародна співпраця, моніторинг інцидентів, спроможність раннього попередження та сповіщення, реагування на інциденти, аналіз ризиків та ситуативна обізнаність, співпраця з приватним сектором, стандартний порядок дій тощо.	1				
4					Чи існує механізм співпраці з іншими сусідніми країнами щодо інцидентів?	1				

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
5					Чи формалізовано чітку політику та процедури щодо обробки інцидентів?	1				
6					Чи беруть участь національні команди CSIRT у тренуваннях із кібербезпеки як на національному, так і на міжнародному рівнях?	1				
7					Чи долучена національна команда CSIRT до FIRST (Форум команд реагування на інциденти та забезпечення безпеки)?	0				

Рекомендації

✓ рішенням НКЦК зобов'язати суб'єктів кіберзахисту проводити не рідше ніж раз на рік оцінку відповідності всіх протоколів реагування на кіберінциденти, а також перевіряти їхню дієвість та функціональність (рівень 5).

Ціль 5 - підвищити обізнаність користувачів

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) з чітким розподілом ресурсів та управлінням ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи існує мінімальне визнання з боку уряду, приватного сектору або загальних користувачів, що існує потреба підвищити обізнаність щодо питань кібербезпеки та конфіденційності?	1	Чи визначено конкретну цільову аудиторію для підвищення обізнаності користувачів? Наприклад, загальні користувачі, молодь, бізнес-користувачі (малий та середній бізнес, оператори основних послуг, оператори цифрових послуг тощо).	1	Чи розроблено комунікаційні плани / стратегію для кампаній?	1	Чи складено метрики для оцінки національної кампанії на етапі планування?	1	Чи запроваджені механізми для забезпечення постійної актуальності кампаній із підвищення обізнаності з огляду на технологічний прогрес, зміни в середовищі загроз, правові норми та директиви з національної безпеки?	1
2	Чи проводять державні установи інформаційні кампанії з питань кібербезпеки в межах своєї організації за умов необхідності? Наприклад, після інциденту з кібербезпекою.	0	Чи готується план заходів щодо підвищення обізнаності з питань інформаційної безпеки та конфіденційності даних?	1	Чи існує процес створення контенту, спрямованого на підвищення рівня кібергігієни на державному рівні?	1	Чи оцінюється спроможність реагувати на інциденти, аби переконатися, що у вас достатньо ресурсів та навичок для виконання завдань, викладених у пункті (2) Додатку I Директиви NIS?	1	Чи проводиться оцінка кампаній після їхнього виконання?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
3	Чи проводять державні установи інформаційні кампанії з питань кібербезпеки для широкої громадськості за умов виникнення необхідності? Наприклад, після інциденту з кібербезпекою.	0	Чи є в держави доступні та легко впізнавані ресурси(наприклад, єдиний інтернет-портал, набір інструментів з підвищення обізнаності) для користувачів, які прагнуть засвоїти інформацію щодо питань кібербезпеки та конфіденційності?	1	Чи існують механізми для визначення тих цільових груп, які потребують першочергового підвищення кіберобізнаності (як-от Оцінка середовища загроз ENISA, звіти національних центрів боротьби з кіберзлочинністю тощо)?	1	Чи запроваджені будь-які механізми для визначення найбільш відповідних засобів масової інформації чи каналів комунікації залежно від цільової аудиторії з метою максимального охоплення та залучення? Наприклад, різні типи цифрових медіа, брошури, електронні листи, навчальний матеріал, плакати в людних місцях, телебачення, радіо тощо.	1	Чи проводяться консультації з поведінковими експертами, аби адаптувати комунікаційну кампанію до цільової аудиторії?	1
4					Чи існує практика збирання разом зацікавлених осіб з експертами та командами комунікацій для створення контенту?	1				
5					Чи залучається приватний сектор до діяльності в рамках інформаційних кампаній і поширення повідомлень серед ширшої аудиторії?	1				
6					Чи готуються конкретні ініціативи щодо підвищення обізнаності	1				

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
6					для керівників державного, приватного, академічного або громадськогосекторів?	1				
7					Чи проводяться заходи в межах щорічних місячників кібербезпеки?	0				

Рекомендації

✓ відповідальним за тематичні пункти суб'єктам реалізації Стратегії кібербезпеки доцільно сформувати робочу групу для розробки Національної програми підвищення кіберобізнаності / кіберграмотності (рекомендується під час її розробки використовувати матеріали AR-in-the-box ENISA);

✓ передбачити, що Національна програма має містити таке: метрики її виконання, процедуру регулярної (щонайменше раз на рік) оцінки ефективності її реалізації, чітко визначені та пріоритезовані цільові групи для підвищення кіберобізнаності (останні мають переглядатися протягом виконання всієї Нацпрограми, базуючись на оцінках ландшафту кіберзагроз), визначені основні канали комунікації щодо формування кіберобізнаності;

✓ Нацпрограма має містити постійно (раз на рік) оновлюваний комунікаційний план: основні ідеї інформаційної кампанії, шляхи їхньої реалізації та очікувані показники охоплення;

✓ після розробки та затвердження Нацпрограми доцільно утворити при основному відповідальному за її реалізацію органі постійно чинну групу з числа представників державних структур, експертів з комунікації (з обов'язковим включенням поведінкових експертів) та приватного сектору задля постійної оцінки ефективності реалізації Нацпрограми та надання пропозицій щодо її оптимізації.

Ціль 6 - організувати тренування з кібербезпеки

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) з чітким розподілом ресурсів та управлінням ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи проводяться кризові тренування в інших секторах (крім кібербезпеки) на національному рівні?	1	Чи існує програма тренування з кібербезпеки на національному рівні?	1	Чи залучаються всі відповідні органи державного управління? (навіть якщо сценарій притаманний певному сектору)	1	Чи пишуться звіти після закінчення дій / звіти про оцінку?	1	Чи наявна спроможність проводити аналіз надбаного досвіду в кіберсфері (процеси звітування, аналіз, пом'якшення наслідків)?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
2	Чи наявні ресурси, виділені для розробки та планування навчання з управління кризовими ситуаціями?	1	Чи проводяться тренування з управління кіберкризами щодо життєво важливих соціальних функцій та критично важливої інфраструктури?	1	Чи залучається приватний сектор до планування та виконання тренувань?	1	Чи проводиться перевірка планів та процедур національного рівня?	1	Чи існує налагоджений процес вивчення уроків?	1
3			Чи визначено координаційний орган для нагляду за розробкою та плануванням тренувань із кібербезпеки (державне агентство, консультування тощо)?	0	Чи організовуються секторальні тренування на національному та/або міжнародному рівні?	1	Чи беруть українські представники участь у тренуваннях з кібербезпеки на загальноєвропейському рівні?	1	Чи адаптується сценарій навчань залежно від останніх надбань (технологічні досягнення, глобальні конфлікти, середовище загроз тощо)?	1
4					Чи є практика організації тренувань у всіх критичних секторах, згаданих у Додатку II до Директиви NIS?	1			Чи узгоджуються процедури управління кризовими ситуаціями з міжнародними партнерами для забезпечення ефективного національного управління кризовими ситуаціями?	1
5					Чи проводяться міжгалузеві тренування з кібербезпеки?	1			Чи впроваджений механізм швидкої адаптації стратегії, планів та процедур з огляду на надбаний досвід після тренувань?	0

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
6					Чи проводяться тренування з кібербезпеки характерні для різних рівнів? (технічний та оперативний рівень, рівень процедури, рівень ухвалення рішень, політичний рівень тощо)	0				

Рекомендації

✓ суб'єктам реалізації Стратегії кібербезпеки під час подання пропозицій до річних планів реалізації Стратегії кібербезпеки закладати видатки на проведення навчальних вправ з персоналом у частині реагування та управління кризовими ситуаціями (рівень 1);

✓ у Національному плані захисту та забезпечення безпеки й стійкості критичної інфраструктури передбачити обов'язкове проведення відповідних тренінгів із реагування та управління кризовими ситуаціями в усіх секторах критичної інфраструктури, загаданих у Законі України «Про критичну інфраструктуру» та постанові Кабінету Міністрів України від 9 жовтня 2020 р. № 1109 (рівень 3);

✓ НКЦК спільно з Державною службою спеціального зв'язку та захисту інформації України сформувати узагальнений план проведення навчань з кібербезпеки та періодично переглядати його на предмет відповідності поточним потребам держави в такому навчанні;

✓ встановити для всіх основних суб'єктів національної системи кібербезпеки та операторів КІ обов'язок брати участь у щонайменше одних ТТХ національного рівня (гібридні загрози та/або секторальні загрози);

✓ передбачити в Національному плані реагування на кіберінциденти обов'язок атакованих організацій та основних суб'єктів національної системи кібербезпеки проводити процедуру «вивчення уроків», а Державній службі спеціального зв'язку та захисту інформації України спільно зі Службою безпеки України та НКЦК розробити типову методику проведення цієї процедури. Визначити обов'язковість внесення змін до об'єктових планів реагування на кіберінцидент з урахуванням «вивчених уроків»;

✓ провести серію консультацій з міжнародними партнерами (наприклад, у форматі двосторонніх діалогів чи відповідно до підписаних Україною міжнародних угод про співробітництво) щодо узгодження спільного реагування на інциденти транскордонного характеру.

Ціль 7 - посилити навчальні та освітні програми

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи розглядають державні органи можливість розробки навчальних та освітніх програм із кібербезпеки?	1	Чи запроваджуються курси, присвячені кібербезпеці?	1	Чи охоплена в Україні культура кібербезпеки на ранній стадії навчального процесу? Наприклад, чи запроваджені курси з кібербезпеки в середній школі та старшій школі?	1	Чи спонукає держава персонал у приватному та державному секторі стати акредитованими або сертифікованими фахівцями?	1	Чи запроваджені механізми, що забезпечують постійну актуальність тренінгів та освітніх програм щодо сучасних та нових технологічних розробок, змін у середовищі	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
1									загроз, правових норм і директив з національної безпеки?	1
2			Чи пропонують українські університети підготовку кандидатів наук у галузі кібербезпеки як самостійну дисципліну, а не як галузь «Інформаційних технологій»?	1	Чи існують в Україні національні дослідницькі лабораторії та освітні установи, які спеціалізуються на кібербезпеці?	1	Чи розроблені в Україні програми навчання або наставництва з питань кібербезпеки для підтримки національних стартапів та малого й середнього бізнесу?	1	Чи створюються академічні центри підвищення кваліфікації в галузі кібербезпеки, які виступають центрами досліджень та освіти?	1
3			Чи існують плани навчання освітян (незалежно від їхньої галузі) з питань інформаційної безпеки та конфіденційності даних? Наприклад, безпека в інтернеті, захист персональних даних, кібербулінг.	1	Чи заохочуються / фінансуються спеціальні курси з питань кібербезпеки та навчальні плани для перепідготовки при центрах зайнятості?	1	Чи існує практика активного сприяння додаванню курсів з інформаційної безпеки в програми вищої освіти не лише для студентів, що вивчають комп'ютерні науки, а й для будь-якої іншої професії та спеціальності? Наприклад, курси з урахуванням потреб певної професії.	1	Чи беруть участь академічні установи в провідних дискусіях у галузі освіти та досліджень з питань кібербезпеки на міжнародному рівні?	0
4					Чи наявні курси та/або спеціалізована програма з кібербезпеки для 5–8 рівнів EQF (Європейська рамка кваліфікацій)?	1	Чи регулярно відбувається оцінка недоліків професійної підготовки (нестачі працівників) у сфері кібербезпеки?	1		

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
5					Чи заохочує держава ініціативи щодо включення курсів безпеки в інтернеті в освіту на початковому та середньому рівнях?	1	Чи є практика сприяння розвитку мереж та обміну інформацією між науковими установами як на національному, так і на міжнародному рівні?	1		
6					Чи є практика фінансування або безплатних базових тренінгів із кібербезпеки для громадян?	0	Чи залучається приватний сектор у будь-якій формі до освітніх ініціатив з питань кібербезпеки? Наприклад, до розробки та проведення курсів, стажування, працевлаштування тощо.	1		
7					Чи організовуються щорічні заходи з кібербезпеки (наприклад, змагання хакерів чи хакатони)?	0	Чи впроваджуються механізми фінансування для заохочення здобуття освітніх / наукових ступенів з кібербезпеки? Наприклад, стипендії, гарантоване стажування / практика, гарантована робота в конкретній галузі або на посадах в державному секторі.	0		

Рекомендації

✓ хоча Стратегія кібербезпеки України вказує на необхідність посилення освітньої складової, однак досі не розроблено й не затверджено чіткої стратегії розвитку освітньої компоненти, відсутнє розуміння ресурсів, які виокремлені для досягнення цього завдання. Міністерству освіти і науки України спільно з основними суб'єктами кібербезпеки, приватним сектором та іншими зацікавленими сторонами доцільно сформувати Національну стратегію розвитку кібербезпекового кадрового потенціалу (рівень 3). Стратегія має передбачати її постійну актуалізацію та корегування напрямів реалізації, конкретний план дій реалізації;

✓ Державною службою зайнятості опрацювати можливість запровадження одним із напрямів перепідготовки кібербезпекові спеціальності (базовані на нових освітніх стандартах кібербезпеки) з метою подальшого підтвердження кваліфікації у відповідних Кваліфікаційних центрах (рівень 3);

✓ Міністерству цифрової трансформації України розробити курси кібербезпеки з акцентом на малий та середній бізнес (рівень 4);

✓ Фонду розвитку інновацій (Український фонд стартапів) передбачити за умови видачі грантової допомоги для малого та середнього бізнесу обов'язкову вимогу до грантоотримувачів у вигляді підтвердженого проходження відповідних освітніх заходів Міністерства цифрової трансформації України (рівень 4);

✓ Міністерству освіти і науки України рекомендувати вищим навчальним закладам усіх форм власності додати в освітні програми підготовки фахівців за всіма напрямками щонайменше короткі тематичні (пов'язані із конкретним фахом) курси кібербезпеки (там, де це доцільно: захист інформації, робота з персональними даними тощо) (рівень 4);

✓ Міністерству освіти і науки України започаткувати загальноукраїнську експертну оцінку (у вигляді річного звіту з рекомендаціями) щодо оцінки недоліків професійної підготовки в сфері кібербезпеки. Оцінка має містити конкретні пропозиції щодо поліпшення освітніх / тренінгових програм на базі актуальних викликів кібербезпеці України, а також прогнозних оцінок таких викликів (рівень 4 та 5).

Ціль 8 - сприяти науково-дослідним і дослідно-конструкторським роботам

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи проводилися дослідження або аналізи для визначення пріоритетів НДДКР у галузі кібербезпеки?	1	Чи створено процес визначення пріоритетів НДДКР в сфері кібербезпеки (наприклад, нові можливості для стримування, захисту, виявлення та адаптації до нових видів кібератак)?	1	Чи існує розуміння на рівні держави як пов'язати проєкти НДДКР з реальною економікою?	1	Чи відповідають проєкти НДДКР з кібербезпеки відповідним стратегічним цілям, наприклад, Стратегії кібербезпеки України?	1	Чи здійснює Україна співпрацю на національному рівні з будь-якими міжнародними проєктами НДДКР, пов'язаними з кібербезпекою?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
2			Чи бере участь приватний сектор у формуванні пріоритетів НДДКР?	1	Чи існують національні проєкти, пов'язані з кібербезпекою?	1	Чи існує схема оцінки для проєктів НДДКР?	1	Чи узгоджуються пріоритети НДДКР з чинним або майбутнім нормативно-правовим регулюванням (національний рівень)?	1
3			Чи беруть участь наукові кола у формуванні пріоритетів НДДКР?	1	Чи є в Україні місцеві / регіональні екосистеми стартапів та інші канали взаємодії (наприклад, технологічні парки, інноваційні кластери, події / платформи з нетворкінгу) для сприяння інноваціям зокрема для стартапів із кібербезпеки)?	1	Чи існують угоди про співпрацю між державними органами та університетами, іншими науково-дослідними установами?	1	Чи долучена Україна до участі в провідних дискусіях з однієї чи багатьох передових тем НДДКР на міжнародному рівні?	0
4			Чи існують національні проєкти НДДКР, пов'язані з кібербезпекою?	0	Чи інвестуються кошти в програми НДДКР у галузі кібербезпеки в наукових колах і приватному секторі?	1	Чи є визнаний інституційний орган, який наглядає за науково-дослідною діяльністю в галузі кібербезпеки?	0		
5					Чи існують центри науково-промислових досліджень в університетах, аби поєднувати теми досліджень і потреби ринку?	1				

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
6					Чи існують спеціальні програми фінансування НДДКР у сфері кібербезпеки?	0				

Рекомендації

✓ НАН України доцільно у разі затвердження НДДКР, що пов'язані з різними аспектами кібербезпеки, вимагати від авторів вказувати, який вплив ці НДДКР матимуть на реальну економіку. НКЦК доцільно створити окрему робочу групу для періодичних консультацій із представниками наукового співтовариства, які займаються відповідними кібербезпековими НДДКР, з метою підвищення якості координації дослідницьких процесів та ліпшого розуміння очікуваного впливу результатів НДДКР на економіку та сферу кібербезпеки (рівень 3);

✓ НАН України розробити та затвердити методику оцінки проєктів НДДКР, що мають безпосередній зв'язок зі сферою кібербезпеки. Оцінка має містити рейтингування проєктів з погляду їхньої важливості, виду (фундаментальні / прикладні), сфери спрямування тощо. Надалі результати цієї оцінки можуть використовуватися державними органами під час формування видатків на наукові дослідження в сфері кібербезпеки, а також пошуку додаткових коштів міжнародної допомоги для їхньої реалізації (рівень 4);

✓ НКЦК спільно з НАН України визначити (а в разі потреби створити) орган (можливо, у формі постійно чинної міжвідомчої групи), який буде здійснювати нагляд за науково-дослідною діяльністю в галузі кібербезпеки.

Ціль 9 - забезпечити стимули для приватного сектору інвестувати в заходи безпеки

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи існує чинна промислова політика або політична воля для заохочення розвитку галузі кібербезпеки?	1	Чи бере участь приватний сектор у розробці стимулів до розвитку сфери кібербезпеки?	1	Чи впроваджені економічні, регуляторні або інші види стимулів для сприяння інвестиціям у кібербезпеку?	1	Чи є приватні суб'єкти, які реагують на заохочення, інвестуючи в заходи безпеки? Наприклад, інвестори, що спеціалізуються на кібербезпеці, та неспеціалізовані інвестори.	1	Чи акцентує держава увагу на ініціативах із питань кібербезпеки відповідно до останніх подій, пов'язаних із загрозами?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
2			Чи визначено конкретні складові / напрями кібербезпеки, які слід розробляти? Наприклад, криптографія, приватність, нова форма автентифікації, ШІ для кібербезпеки тощо.	0	Чи надається підтримка (наприклад, податкові пільги) для стартапів і МСП, що займаються кібербезпекою?	1	Чи стимулює держава приватний сектор зосередитися на безпеці передових технологій? Наприклад, 5G, штучний інтелект, інтернет-продукти, квантові обчислення тощо.	1		
3					Чи надаються податкові пільги або інша фінансова мотивація інвесторам приватного сектору в стартапах із кібербезпеки?	1				
4					Чи сприяє держава доступу стартапам і МСП, що займаються кібербезпекою, до процесу державних закупівель?	0				
5					Чи наявний у держави бюджет для стимулювання приватного сектору?	0				

Рекомендації

✓ на нормативно-правовому рівні зокрема через закон, що визначатиме основні засади розвитку інформаційного суспільства, Бюджетний кодекс України тощо) визначити таке: ключові види економічних, регуляторних або інших видів

стимулів для сприяння інвестиціям у кібербезпеку; заходи підтримки (наприклад, податкові пільги) для стартапів і малого та середнього бізнесу (МСБ), що займаються кібербезпекою; податкові пільги або інша фінансова мотивація для інвесторів приватного сектору, що підтримують стартапи з кібербезпеки; можливі заходи сприяння держави для кращого доступу стартапів і МСБ, що займаються кібербезпекою, до процесу державних закупівель; заходи бюджетного стимулювання приватного сектору щодо розвитку кібербезпеки. Заходи стимулювання мають також передбачати окремий фокус уваги на кібербезпеці передових технологій, як-от 5G, штучний інтелект, інтернет-продукти, квантові обчислення тощо (рівень 4);

✓ щорічно проводити огляд стану виконання та ефективності цих стимулів із поданням пропозицій щодо їхнього перегляду / модернізації. Вказаний огляд доцільно готувати за прямого залучення представників приватного сектору, що або працюють у сфері кібербезпеки, або інвестують у таку діяльність (рівень 5).

Ціль 10 - покращити кібербезпеку ланцюга постачання

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи проводилися дослідження кращих практик безпеки в галузі управління ланцюгами постачання, що використовуються для закупівель у різних сегментах	1	Чи проводяться оцінки кібербезпеки по всьому ланцюгу постачання сервісів і продуктів ІКТ у критично важливих секторах (як зазначено в Додатку II до Директиви NIS (2016/1148))?	1	Чи використовується схема сертифікації безпеки для продуктів і сервісів, заснованих на ІКТ? Наприклад, такі як європейська Угода про визнання спільних критеріїв (CCRA),	1	Чи запроваджений процес оновлення оцінок кібербезпеки в ланцюзі постачання сервісів і продуктів ІКТ у критично важливих секторах (як зазначено в Додатку II Директиви NIS	1	Чи існують детекторні зонди в ключових елементах ланцюга постачання для виявлення ранніх ознак порушення нормального функціонування? Наприклад, контроль	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
1	промисловості та/або в державному секторі?	1		1	національні проєкти, галузеві проєкти тощо.	1	(2016/1148))?	1	безпеки на рівні інтернет-провайдера, зонди безпеки в основних компонентах інфраструктури тощо.	1
2			Чи застосовуються стандарти в політиці закупівель державних адміністративних органів, аби гарантувати, що постачальники продуктів або сервісів ІКТ відповідають базовим вимогам щодо інформаційної безпеки? Наприклад, ISO/IEC 27001 та 27002, ISO/IEC 27036 тощо.	1	Чи держава активно сприяє безпеці та конфіденційності даних, створюючи передові практики розробки продуктів і сервісів ІКТ? Наприклад, безпечний життєвий цикл розробки програмного забезпечення, життєвий цикл інтернет-продуктів.	1	Чи запроваджений процес виявлення слабких ланок кібербезпеки в ланцюгу постачання критично важливих секторів (як визначено в Додатку II до Директиви NIS (2016/1148))?	1		
3					Чи розроблюються та надаються централізовані каталоги з розширеною інформацією про наявні стандарти інформаційної безпеки та конфіденційності, які є масштабованими для МСП та застосовуються ними?	1	Чи запроваджені механізми, які гарантують, що критично важливі для операторів основних послуг продукти та сервіси ІКТ є кіберстійкими (тобто здатні підтримувати доступність та безпеку від кіберінцидентів)? Наприклад, шляхом тестування, регулярних оцінок, виявлення ушкоджених елементів тощо.	1		

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
4					Чи бере держава участь у розробці Керівництва ЄС з сертифікації цифрових продуктів, сервісів і процесів ІКТ?	0	Чи сприяє держава розробці схем сертифікації, орієнтованих на малий та середній бізнес, для підвищення інформаційної безпеки та прийняття стандартів конфіденційності?	0		
5					Чи надаються малому та середньому бізнесу будь-які види стимулів із метою ухвалення ними стандартів безпеки та конфіденційності?	0	Чи розроблені будь-які положення, що заохочують великі компанії збільшувати кібербезпеку малих підприємств у своїх ланцюгах постачання? Наприклад, інтернет-вузол кібербезпеки, навчальні та інформаційні кампанії тощо.	0		
6					Чи заохочуються постачальники програмного забезпечення підтримувати малий та середній бізнес через більш безпечні конфігурації за налаштуванням у продуктах, орієнтованих на невеликі організації?	0				

Рекомендації

✓ передбачити в оновленій Стратегії кібербезпеки України окремий розділ щодо безпеки ланцюжків постачання з відповідними завданнями у Плані дій з реалізації Стратегії;

✓ НКЦК ініціювати проведення експертного дослідження щодо кращих практик безпеки в галузі управління ланцюжками постачання, які використовуються в сфері закупівель у різних сегментах промисловості та/або в державному секторі провідних країн світу;

✓ НКЦК ініціювати проведення експертного дослідження щодо оцінки безпеки ланцюжків постачання відповідно до переліку секторів критичної інфраструктури, визначених Законом України «Про критичну інфраструктуру» та постановою Кабінету Міністрів України від 9 жовтня 2020 р. № 1109. За результатами дослідження спільно з суб'єктами кібербезпеки провести оцінку кібербезпеки в ланцюзі постачання сервісів і продуктів ІКТ у критично важливих секторах;

✓ доцільно розглянути необхідність введення системи звітування ОКІ (щонайменше 1-2 категорії) перед визначеним державним органом про ключові елементи ланцюжків постачання, щодо яких ОКІ відстежує можливі порушення та які заходи вживає для недопущення атак через такі елементи. Наприклад, зробити це частиною паспорту ОКІ;

✓ Держспецзв'язку України спільно з іншими уповноваженими органами розробити та опублікувати настанови щодо документування ланцюжків постачання організацій, основні методи їхнього захисту (безпеки) та тестування. Ці настанови мають бути сегментовані за цільовими аудиторіями: МСБ, оператори КІ та державні структури;

✓ встановити обов'язкові вимоги оцінки стану кібербезпеки для організацій, що є постачальниками послуг для ОКІ 1-2 категорій;

✓ НКЦК спільно з Держспецзв'язком України ініціювати дослідження щодо можливості приєднання України до Європейської рамки з сертифікації цифрових продуктів, сервісів і процесів ІКТ, та за можливості розпочати діалог з уповноваженими структурами ЄС щодо приєднання до цього процесу;

✓ спільно з представниками компаній великого бізнесу опрацювати питання встановлення з їхнього боку додаткових заохочувальних (чи обмежувальних) заходів для малих постачальників (МСБ) з метою дотримання ними вимог кібербезпеки. Оцінити можливість надання додаткових стимулів для організацій великого бізнесу щодо запровадження ними підвищених вимог кібербезпеки до їхніх постачальників;

✓ спільно з постачальниками програмного забезпечення, яке активно використовується МСБ, опрацювати можливість створення для таких суб'єктів додаткових спеціальних програм підтримки щодо посилення їхньої кібербезпеки.

Ціль 11 - захист критичної інформаційної інфраструктури (KII), операторів основних послуг і провайдерів цифрових послуг

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи є загальне розуміння того, що оператори KII сприяють національній безпеці?	1	Чи існує у вас методологія визначення основних послуг?	1	Чи впроваджено Директиву NIS (2016/1148)?	1	Чи існує процедура оновлення реєстру ризиків?	1	Чи створюються та оновлюються звіти про середовище загроз?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
2			Чи існує методологія ідентифікації КІІ?	1	Чи впроваджено Директиву ЕСІ (2008/114) про ідентифікацію та позначення європейських критичних інфраструктур та оцінку необхідності вдосконалення їхнього захисту?	1	Чи запроваджено інші механізми, що дозволяють виміряти, чи технічні й організаційні заходи, впроваджені операторами основних послуг, які є адекватними для управління ризиками, що стоять перед безпекою мережі та інформаційних систем? Наприклад, регулярні аудити кібербезпеки, національне керівництво для впровадження стандартних заходів, технічні інструменти, що надаються урядом, як-от детекторні зонди або аналіз конфігурації для конкретної системи тощо.	1	Залежно від останніх подій у середовищі загроз чи існує можливість включити новий сектор у національний план дій щодо захисту КІІ?	1
3			Чи існує методологія визначення операторів основних послуг?	1	Чи існує національний реєстр операторів основних послуг у кожному з критичних секторів?	1	Чи аналізується та, відповідно, оновлюється перелік визначених операторів основних послуг щонайменше раз на два роки?	1	Залежно від останніх подій у середовищі загроз чи існує можливість внести нові вимоги в план дій щодо захисту КІІ?	1
4			Чи існує методологія визначення постачальників цифрових послуг?	1	Чи існує національний реєстр визначених постачальників цифрових послуг?	1	Чи запроваджені механізми, що дозволяють виміряти, чи технічні й організаційні	1		

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
4							заходи, впроваджені постачальниками цифрових послуг, які є адекватними для управління ризиками, що стоять перед безпекою мережі та інформаційних систем? Наприклад, регулярні аудити кібербезпеки, національне керівництво для впровадження стандартних заходів, технічні інструменти, що надаються урядом, як-от детекторні зонди або аналіз конфігурації для конкретної системи тощо.	1		
5			Чи існує один або кілька національних органів, що здійснюють нагляд за захистом критично важливої інформаційної інфраструктури та безпекою мережі та інформаційних систем? Наприклад, відповідно до вимог Директиви NIS (2016/1148).	1	Чи існує національний реєстр ризиків для виявлених або відомих ризиків?	1	Чи аналізується та, відповідно, оновлюється перелік визначених постачальників цифрових послуг щонайменше раз на два роки?	1		
6			Чи розроблюються секторальні плани захисту? Наприклад,	0	Чи існує методологія картографування взаємозалежностей KII?	1	Чи використовується схема сертифікації безпеки (національна	1		

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
6			базові заходи з кібербезпеки (обов'язкові або настанови).	0		1	або міжнародна), аби допомогти операторам основних послуг та постачальникам цифрових послуг ідентифікувати безпечні продукти ІКТ?	1		
7					Чи застосовується практика управління ризиками для виявлення, кількісного визначення та управління ризиками, пов'язаними з КІІ, на національному рівні?	1	Чи використовується схема сертифікації безпеки або процедура кваліфікації для оцінки постачальників послуг, які працюють з операторами основних послуг? Наприклад, постачальники послуг у сфері виявлення інцидентів, реагування на інциденти, аудит кібербезпеки, хмарні сервіси, комп'ютеризовані карти тощо.	1		
8					Чи бере Україна участь у консультаційному процесі для виявлення транскордонних взаємозалежностей?	1	Чи запроваджено механізми для вимірювання рівня відповідності операторів основних послуг та постачальників цифрових послуг з огляду дотримання базових заходів кібербезпеки?	0		

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
9					Чи існує єдиний координатор, відповідальний за координацію питань, що стосуються безпеки мережевих та інформаційних систем на національному рівні та в рамках транскордонного співробітництва?	1	Чи ухвалені розпорядження щодо забезпечення безперервності сервісів, які надаються критично важливими інформаційними інфраструктурами? Наприклад, передбачення кризи, процедури відновлення критично важливих інформаційних систем, безперервність бізнесу без IT, процедури резервного копіювання й переміщення даних у режим офлайн тощо.	0		
10					Чи визначено базові заходи з кібербезпеки (обов'язкові або настанови) для постачальників цифрових послуг та всіх секторів, визначених у Додатку II до Директиви NIS (2016/1148)?	1				
11					Чи надаються інструменти або методології для виявлення кіберінцидентів?	0				

Рекомендації

✓ створити Національний реєстр ризиків, а також затвердити процедуру його постійного оновлення;

✓ Держспецзв'язку України розробити методологію, а на її основі проводити періодичне дослідження щодо картографування взаємозалежностей КІІ. На базі вказаного дослідження розпочати діалог з європейськими партнерами щодо вивчення аналогічних транскордонних взаємозалежностей;

✓ започаткувати щорічний зведений публічний звіт про середовище загроз (бажано за методологією ENISA);

✓ НКЦК та Держспецзв'язку України розпочати діалог з ENISA (як розробником методології оцінки рівня національних спроможностей) щодо модернізації методології в частині імплементації положень NIS Директиви та заміни вказаних завдань на впровадження Директив 2555/2557;

✓ опрацювати доцільність введення процедури сертифікації для тих постачальників послуг, що безпосередньо працюють з ОКІ (зокрема постачальники послуг кібербезпеки);

✓ запровадити обов'язкові вимоги щодо наявності в усіх ОКІ Business Contingency Plans. Держспецзв'язку України спільно з іншими основними суб'єктами розробити типові плани та методику їхнього застосування.

Ціль 12 - протидія кіберзлочинності

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи проводилися дослідження з метою виявлення стану спроможностей правоохоронних органів (правової бази, ресурсів, навичок тощо)	1	Чи повністю відповідає національна законодавча база відповідній законодавчій базі ЄС, включно з Директивою 2013/40/ЄС про атаки на	1	Чи є в країні підрозділи, відповідальні за протидію кіберзлочинності в органах прокуратури?	1	Чи збирається статистика згідно з положеннями статті 14 (1) Директиви 2013/40/ЄС (Директива про атаки на інформаційні системи)?	1	Чи існує міжвідомче навчання або тренінги для представників правоохоронних органів, суддів, прокурорів і національних /	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
1	для ефективного подолання кіберзлочинності?	1	інформаційні системи? Наприклад, незаконний доступ до інформаційних систем, незаконне втручання в систему, незаконне втручання в дані, незаконне перехоплення, інструменти, що використовуються для вчинення правопорушень тощо.	1		1		1	державних команд CSIRT на національному рівні та/або на багатосторонньому рівні?	1
2	Чи проводились дослідження з метою виявлення вимог до прокурорів і суддів (правової бази, ресурсів, навичок тощо) для ефективного подолання кіберзлочинності?	1	Чи існує будь-яке законодавче положення, що стосується крадіжки особистих даних в інтернеті та крадіжки персональних даних?	1	Чи існує спеціальний бюджет, виділений підрозділам з питань протидії кіберзлочинності?	1	Чи збирається окрема статистику щодо кіберзлочинності? Наприклад, оперативна статистика, статистика тенденцій кіберзлочинності, статистика доходів від кіберзлочинності та завданих збитків тощо.	1	Чи бере Україна участь у скоординованих діях на міжнародному рівні з метою зриву злочинної діяльності? Наприклад, проникнення на злочинні форуми хакерів, в організовані групи кіберзлочинців, на темні вебринки та ліквідація ботнетів тощо.	1
3	Чи підписала Україна Будапештську конвенцію Ради Європи про кіберзлочинність?	1	Чи існують які-небудь юридичні положення, що стосуються порушення інтелектуальної власності та авторського права в інтернеті?	1	Чи створено центральний орган / організацію для координації діяльності в сфері боротьби з кіберзлочинністю?	1	Чи оцінюється адекватність тренінгів для представників правоохоронних органів, судової влади та персоналу національної команди CSIRT з питань боротьби з кіберзлочинністю?	1	Чи існує чіткий розподіл обов'язків між командою CSIRT, правоохоронними органами та органами правосуддя (прокурорами та суддями), коли вони співпрацюють з метою подолання кіберзлочинів?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
4			Чи існують які-небудь законодавчі положення, що стосуються переслідувань в інтернеті чи кібербулінгу?	1	Чи встановлено механізми співпраці між відповідними національними установами, які залучені до боротьби з кіберзлочинністю, зокнрема між правоохоронними органами, національними командами CSIRT?	1	Чи регулярно проводяться оцінки, аби переконатися, що в країни є достатньо ресурсів (людських, бюджетних та інструментальних), виділених для підрозділів з питань кіберзлочинності в межах правоохоронної системи?	1	Чи сприяє нормативна база співпраці між командами CSIRT / правоохоронними органами та органами правосуддя (прокурорами та суддями)?	1
5			Чи існує будь-яке законодавче положення щодо боротьби з комп'ютерним шахрайством? Наприклад, дотримання положень Будапештської конвенції Ради Європи про кіберзлочинність.	1	Чи існує співпраця та обмін інформацією з країнами-членами ЄС у сфері боротьби з кіберзлочинністю?	1	Чи регулярно проводяться оцінки, аби переконатися, що в країни є достатньо ресурсів (людських, бюджетних та інструментальних), виділених для підрозділів з питань кіберзлочинності в межах органів прокуратури?	1	Чи бере Україна участь у створенні та підтримці стандартизованих інструментів і методологій, форм і процедур, якими можна ділитися із міжнародними партнерами (правоохоронними органами, командами CSIRT, ENISA, EC3 Європолу тощо)?	1
6			Чи існує будь-яке законодавче положення щодо захисту дітей в інтернеті? Наприклад, дотримання положень Директиви 2011/93/ЄС та Будапештської конвенції Ради Європи про кіберзлочинність.	1	Чи Україна співпрацює та обмінюється інформацією з агентствами ЄС (наприклад, Європолом EC3, Євроюстом, ENISA) у сфері боротьби з кіберзлочинністю?	1	Чи існують підрозділи, спеціалізовані суди або судді, які розглядають справи про кіберзлочини?	1	Чи існують якісь прогресивні механізми, що утримують людей від залучення до кіберзлочинів чи участі в них?	0

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
7			Чи визначено оперативного національного координатора для обміну інформацією та реагування на термінові інформаційні запити країн-членів ЄС щодо правопорушень, визначених Директивою 2013/40/ЄС (Директива про атаки на інформаційні системи)?	1	Чи існують належні інструменти для боротьби з кіберзлочинністю? Наприклад, таксономія та класифікація кіберзлочинів, інструменти для збору електронних доказів, інструменти комп'ютерної криміналістики, надійні платформи обміну тощо.	1	Чи існують якісь розпорядження щодо надання підтримки та допомоги жертвам кіберзлочинів (загальні користувачі, малий та середній бізнес, великі компанії)?	1	Чи використовує Україна Концепцію та/або Протокол ЄС щодо реагування на надзвичайні ситуації правоохоронних органів (EU LE ERP) для ефективного реагування на широкомасштабні кіберінциденти?	0
8			Чи входить до структури національного правоохоронного органу спеціальний підрозділ з питань кіберзлочинності?	1	Чи існують стандартні операційні процедури для обробки електронних доказів?	1	Чи встановлено міжвідомчу базу та механізми співпраці між усіма відповідними зацікавленими особами (наприклад, правоохоронними органами, національною командою CSIRT, органами правосуддя, спільнотою), зокрема приватним сектором (наприклад, операторами основних послуг, постачальниками сервісів), де це доречно, для реагування на кібератаки?	1		
9			Чи призначено відповідно до ст. 35	1	Чи бере Україна участь у можливостях	0	Чи сприяє українська нормативна база	1		

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
			Будапештської конвенції цілодобового координатора?		підвищення кваліфікації, які пропонують та/або підтримують агентства ЄС (наприклад, Європол, Євроюст, Європейське бюро з боротьби з шахрайством, Європейський поліцейський коледж Cepol, ENISA)?		співпраці між командами CSIRT та правоохоронними органами?			
10		1	Чи призначено оперативного цілодобового національного координатора для Протоколу ЄС щодо реагування на надзвичайні ситуації правоохоронних органів (EU LE ERP) для реагування на великі кібератаки?	1	Чи планує Україна ухвалити 2-ий додатковий протокол до Будапештської конвенції Ради Європи про кіберзлочинність?	0	Чи запроваджено механізми (наприклад, інструменти, процедури) для полегшення обміну інформацією та співпраці між командами CSIRT / правоохоронними органами та, можливо, органами правосуддя (прокурорами та суддями) в сфері боротьби з кіберзлочинністю?	1		
11			Чи проводиться регулярно спеціалізоване навчання для зацікавлених осіб, які беруть участь у протидії кіберзлочинності (для правоохоронних органів, органів правосуддя, команди CSIRT)? Наприклад, серед	1						

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
			іншого, тренінги з питань реєстрації / переслідування злочинів у кіберпросторі, тренінги зі збору електронних доказів та забезпечення цілісності в усьому цифровому ланцюзі арешту та комп'ютерної криміналістики.							
12			Чи ратифікувала / приєдналася Україна до Будапештської конвенції Ради Європи про кіберзлочинність?	1						
13			Чи підписала та ратифікувала Україна Додатковий протокол (криміналізація актів расистського та ксенофобського характеру, вчинених за допомогою комп'ютерних систем) до Будапештської конвенції Ради Європи про кіберзлочинність?	0						

Рекомендації

✓ розглянути можливість створення спеціалізованих судів (або додатково підготовлених суддів), що займаються розглядом справ про кіберзлочини (рівень 4);

✓ проводити на регулярній основі інформаційні кампанії щодо запобігання залучення громадян у кіберзлочинну діяльність.

Ціль 13 - встановити механізми звітування про інциденти

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи існують неформальні механізми обміну інформацією щодо інцидентів у сфері кібербезпеки між приватними організаціями та органами влади?	1	Чи існує схема звітування про інциденти для всіх секторів згідно з Додатком II до Директиви NIS?	1	Чи існує схема обов'язкового звітування про інциденти, яка функціонує на практиці?	1	Чи існує гармонізована процедура для галузевих схем звітування про інциденти?	1	Чи створюється щорічний звіт про інциденти?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
2			Чи впроваджено вимоги щодо повідомлення для постачальників телекомунікаційних послуг відповідно до статті 40 Директиви (ЄС 2018/1972)? Директива вимагає, аби країни гарантували, що постачальники загальнодоступних електронних мереж передачі даних або загальнодоступних електронних комунікаційних послуг повідомляють без зайвої затримки компетентний орган про інцидент безпеки, який мав значний вплив на функціонування мереж або сервісів.	1	Чи існує механізм координації / співпраці для зобов'язань щодо звітування про інциденти з огляду на Загальний регламент захисту даних GDPR, Директиву NIS, статтю 40 (попередня стаття 13a) та eIDAS?	1	Чи існує схема звітування про інциденти для інших секторів, крім тих, що передбачені Директивою NIS?	1	Чи запроваджено будь-які звіти про середовище кібербезпеки чи інші види аналізу, підготовлені організацією, яка отримує звіти про інциденти?	1
3			Чи запроваджено вимоги щодо повідомлення для постачальників довірчих послуг відповідно до статті (19) Регламенту eIDAS (Регламент (ЄС) No 910/2014)? Стаття (19), серед інших вимог, вимагає, аби	1	Чи існують на національному рівні інструменти для забезпечення конфіденційності та цілісності інформації, що передається через різні канали звітування?	1	Чи вимірюється ефективність процедур звітування про інциденти? Наприклад, показники інцидентів, щодо яких було звітування за допомогою відповідних каналів, час подання звіту про інцидент тощо.	1		

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
3			постачальники довірчих послуг повідомляли наглядовий органу про значні інциденти/порушення.	1		1		1		
4			Чи впроваджено вимоги щодо повідомлення для постачальників цифрових послуг відповідно до статті (16) Директиви NIS? Стаття (16) вимагає, аби постачальники цифрових послуг без надмірної затримки повідомляли компетентний орган або національну команду CSIRT про будь-який інцидент, що суттєво впливає на надання послуги, як зазначено в Додатку III.	1	Чи існує платформа / інструмент для полегшення процесу звітності?	0	Чи існує загальна систематизація на національному рівні для класифікації інцидентів та їхньої категоризації?	0		

Рекомендації

✓ запровадити для постачальників телекомунікаційних послуг обов'язковість повідомлення компетентного органу про інцидент кібербезпеки, який мав значний вплив на функціонування його (постачальника) мереж або сервісів (рівень 2);

✓ започаткувати міжвідомчий механізм координації щодо обов'язкових звітів про інциденти (зокрема інциденти щодо безпеки персональних даних, проблем електронної ідентифікації тощо), які мають надаватись уповноваженим органам (рівень 3);

✓ розробити методологію оцінки ефективності звітування про кіберінциденти, зокрема з вимірюванням формальних показників: часу звітування, використання каналів звітування тощо.

Ціль 14 - посилити захист конфіденційності даних

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи проводилися дослідження або аналіз для виявлення сфер вдосконалення для кращого захисту прав приватності громадян?	1	Чи бере участь національний орган з питань захисту даних у вирішенні питань, пов'язаних з кібербезпекою (наприклад, розробка проєктів нових законів і	1	Чи пропагуються передові практики щодо заходів безпеки та захисту даних спеціально для державного та/або приватного сектору?	1	Чи регулярно проводяться оцінки, аби переконатися, що вкраїни є достатньо ресурсів (людських, бюджетних та інструментальних), призначених для	1	Чи запроваджено механізми для моніторингу останніх технологічних розробок з метою адаптації відповідних настанов і законодавчих положень / зобов'язань?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
1		1	положень про кібербезпеку, визначення мінімальних заходів безпеки)?	1		1	органу з питань захисту даних?	1		1
2	Чи розроблено національну правову базу для забезпечення виконання Загального регламенту про захист даних (Регламент ЄС № 2016/679)? Наприклад, підтримка або введення більш конкретних положень або обмежень до норм Регламенту.	0			Чи запускаються програми з підвищення обізнаності та навчання стосовно цієї теми?	1	Чи заохочуються організації та підприємства проходити сертифікацію на відповідність ISO/IEC 27701:2019 щодо Системи управління інформаційною безпекою конфіденційних даних (СУІБ)?	1	Чи бере Україна активну участь (або сприяє) в проєктах НДДКР щодо технологій підвищення конфіденційності (PET)?	0
3					Чи скоординовано процедури звітування про інциденти з положеннями законодавства в сфері захисту персональних даних?	1				
4					Чи надається сприяння / підтримка розробці технічних стандартів з інформаційної безпеки та конфіденційності? Чи вони спеціально розроблені для малих та середніх підприємств?	0				

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
5					Чи надаються практичні настанови щодо підтримки різних типів контролерів даних стосовно виконання законодавчих вимог та зобов'язань щодо конфіденційності та захисту даних?	0				

Рекомендації

✓ передбачити в оновленій Стратегії кібербезпеки України окремий розділ щодо безпеки персональних даних із відповідними завданнями в Плані дій з реалізації Стратегії;

✓ провести оцінку наявної законодавчої бази та підготувати відповідні зміни до неї для забезпечення виконання Загального регламенту про захист даних (Регламент ЄС № 2016/679) (рівень 1);

✓ здійснити необхідні кроки, аби процедури звітування про кіберінциденти враховували й необхідність звітування про інциденти з втратою персональних даних у випадку таких інцидентів;

✓ Уповноваженому Верховної Ради України з прав людини проводити щорічну оцінку ситуації із захистом персональних даних (зокрема щодо достатності в державних органів ресурсів на таку діяльність) в державному секторі;

✓ під час оновлення законодавства щодо побудов систем захисту даних (зокрема системи управління інформаційною безпекою) передбачити обов'язкове врахування в них основних положень та вимог ISO/IEC 27701:2019;

✓ НАН України спільно з іншими зацікавленими сторонами впровадити дослідницькі програми, спрямовані на розвиток PET (privacy enhancing technologies) зокрема, але не обмежуючись end-to-end шифруваннями, VPN тощо.

Ціль 15 - встановити державно-приватне партнерство (ДПП)

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи загальноприйнято на рівні країни, що ДПП сприяє підвищенню рівня кібербезпеки в країні за допомогою різних засобів? Наприклад, спільні дії на базі спільних інтересів	1	Чи існує національний план дій щодо встановлення ДПП?	1	Чи є конкретні приклади державно-приватного партнерства на національному рівні?	1	Чи є конкретні приклади міжгалузевого ДПП?	1	Залежно від останніх технологічних та регуляторних розробок чи можете ви адаптувати або створити ДПП?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
1	для зростання галузі кібербезпеки, співпраця у створенні відповідної нормативної бази з питань кібербезпеки, сприяння НДДКР тощо.	1		1		1		1		1
2			Чи визначено юридичну або договірну основу (конкретні закони, договори про нерозголошення, інтелектуальну власність) для охоплення сфери ДПП?	1	Чи існують конкретні приклади ДПП, які притаманні певній галузі?	1	Чи існують приклади концентрації на механізмах міжвідомчої взаємодії (G2G) та взаємодії між приватними стейкхолдерами (B2B) в рамках наявних механізмів ДПП?	1		
3					Чи здійснює держава фінансування конкретних елементів ДПП?	1	Чи існує сприяння створенню ДПП серед малих і середніх підприємств?	1		
4					Чи загалом державні установи очолюють процес створення ДПП? Тобто чи існує єдиний координатор із державного сектору, який керує та координує ДПП, чи державні органи заздалегідь домовляються про те, чого вони хочуть	1	Чи вимірюються результати ДПП?	1		

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
4					досягти, чи є чіткі настанови від державних адміністративних органів щодо їхніх потреб та обмеження для приватного сектору тощо.	1				
5					Чи є Україна (державні органи) членом міжнародних організацій, метою яких є просування ДПП? Наприклад, Європейської організації з кібербезпеки (ECSO) чи інших подібних структур.	0				
6					Чи існує в Україні одне або кілька ДПП, що працюють у рамках діяльності команди CSIRT?	0				
7					Чи існує в Україні одне або кілька ДПП, що працюють над питаннями захисту критично важливої інформаційної інфраструктури?	0				

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
8					Чи існує в Україні одне або кілька ДПП, що працюють над підвищенням рівня обізнаності та розвитку навичок у сфері кібербезпеки?	0				

Рекомендації

✓ розробити за ухвалити закон про державно-приватне партнерство в сфері кібербезпеки, а також Національну стратегію ДПП для практичної реалізації положень закону. Закон також має визначити конкретні юридичні форми ДПП в сфері кібербезпеки та логіку реалізації таких проєктів. (рівень 2). Національна стратегія має окремо передбачати чіткий та зрозумілий процес залучення МСБ до заходів ДПП;

✓ створити (на базі НКЦК, Держспецзв'язку України або іншого основного суб'єкту національної системи кібербезпеки) загальну базу потреб державних установ у проєктах, що можуть бути реалізовані у форматі ДПП. Державні органи, що планують заходи в сфері ДПП мають передбачати кошти на такі проєкти у своїх бюджетах або отримувати підтвердження можливості залучення таких коштів з боку проєктів міжнародної технічної допомоги (рівень 3);

✓ Національна стратегія має періодично переглядатися. Такий перегляд має відбуватися за участі представників як держави, так і приватного сектору.

Ціль 16 - надати інституційний характер співпраці між державними органами

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						
1	Чи існують неформальні канали співпраці між державними установами?	1	Чи існує національна схема співпраці, орієнтована на кібербезпеку? Наприклад, консультативні ради, координаційні групи,	1	Чи беруть участь органи державної влади в таких схемах співпраці?	1	Чи забезпечуються / створюються канали співпраці в сфері кібербезпеки принаймні між такими державними органами: спецслужбами,	1	Чи надається державним установам узагальнена мінімальна інформація про останні події в середовищі загроз та ситуативна обізнаність щодо кібербезпеки?	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
1		1	форуми, ради, кіберцентри або групи експертів.	1		1	внутрішніми правоохоронними органами, органами прокуратури, урядовими суб'єктами, національною командою CSIRT та військовими?	1		1
2					Чи створено платформи співпраці для обміну інформацією?	1	Чи вимірюються успіхи та обмеження для різних схем співпраці?	1		
3					Чи визначено сферу дії платформи для співпраці (наприклад, завдання та обов'язки, кількість проблемних галузей)?	1				
4					Чи організовуються щорічні зустрічі з метою налагодження співпраці?	1				
5					Чи існує механізми співпраці між компетентними органами на регіональному рівні? Наприклад, мережа фахівців з питань безпеки по регіонах, офіцери з питань кібербезпеки в регіональних Торгово-промислових палатах тощо.	1				

Рекомендації

✓ тим часом як на національному та столичному рівні співпраця між експертами з кібербезпеки здебільшого налагоджена, на регіональному рівні вертикальні та горизонтальні зв'язки все ще недостатні. Важливо створити формат постійних регіональних платформ для фахівців кібербезпеки, на яких вони могли б обговорювати специфічні регіональні проблеми кібербезпеки та консолідовано комунікувати з фахівцями центральних органів влади.

Ціль 17 - долучатися до міжнародної співпраці (не тільки з країнами-членами ЄС)

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
a	Чи охоплює чинна Національна стратегія кібербезпеки завдання розробити Національні плани реагування на інциденти кібербезпеки або чи планується їх включення до майбутньої версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення Цілі в нескоординований спосіб?	1	Чи є в Україні план дій (стосовно Цілі), який офіційно визначений та задокументований?	1	Чи тестується план дій щодо Цілі, аби перевірити ефективність його виконання?	1	Чи є в Україні впроваджені механізми, що забезпечують динамічну адаптацію плану дій щодо Цілі відповідно до змін середовища?	1
b			Чи визначені заплановані результати, керівні принципи або ключові напрями діяльності в плані дій щодо Цілі?	1	Чи має Україна план дій щодо Цілі (або сам Національний план) чіткий розподіл ресурсів та управління ними?	1	Чи переглядається план дій щодо Цілі, аби переконатися, що вона правильно оптимізована й щодо неї правильно визначено пріоритет?	1		
c			Чи розпочато реалізацію плану дій щодо Цілі в рамках хоча б обмеженого обсягу?	0						

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
1	Чи існує стратегія міжнародної взаємодії?	1	Чи має Україна угоди про співпрацю з іншими країнами (двосторонні, багатосторонні) чи партнерами в інших країнах? Наприклад, щодо обміну інформацією, розбудови спроможностей, допомоги тощо.	1	Чи здійснюється обмін інформацією на стратегічному рівні? Наприклад, щодо політик кібербезпеки високого рівня, сприйняття ризику тощо.	1	Чи залучені державні установи з питань кібербезпеки до програм міжнародного співробітництва?	1	Чи ведеться обговорення принаймні однієї або багатьох тем у рамках багатосторонніх угод?	1
2	Чи існують неформальні канали співпраці з іншими країнами?	1	Чи є визначений єдиний координатор, який може виконувати функцію підтримки зв'язку для забезпечення транскордонного співробітництва з державними органами країн-членів (група співпраці, мережа команд CSIRT тощо)?	1	Чи обмінюється Україна інформацією на тактичному рівні? Наприклад, відомості про зловмисників, Центри обміну та аналізу інформації (ISACs), тактика, методи та процедури тощо.	1	Чи регулярно відбувається оцінка результатів проєктів міжнародного співробітництва?	1	Чи ведеться обговорення однієї чи багатьох тем у рамках міжнародних договорів чи конвенцій?	1
3	Чи висловило державне керівництво намір брати участь у міжнародному співробітництві в сфері кібербезпеки?	1	Чи є визначені спеціальні фахівці, які беруть участь у міжнародному співробітництві?	1	Чи обмінюється Україна інформацією на оперативному рівні? Наприклад, інформацією про оперативну координацію, поточні інциденти, контролери IOC тощо.	1			Чи ведуться дискусії або переговори з однієї чи багатьох тем у рамках міжнародних груп експертів? Наприклад, Глобальна комісія зі стабільності кіберпростору (GCSC), Група співпраці ENISA NIS, Група урядових експертів ООН (GGE).	1

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
4					Чи бере участь Україна в міжнародних навчаннях з кібербезпеки?	1				
5					Чи бере участь Україна в міжнародних проєктах щодо розбудови спроможностей? Наприклад, тренінги, програми з розвитку навичок, створення проєктів стандартних процедур тощо.	0				
6					Чи підписано угоди про взаємодопомогу з іншими країнами? Наприклад, діяльність правоохоронних органів, судочинство, поєднання спроможностей реагування на інциденти, спільне використання активів кібербезпеки тощо.	0				
7					Чи підписано або ратифіковано міжнародні договори або конвенції в сфері кібербезпеки? Наприклад, Міжнародний кодекс	1				

	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	R
7					поведінки щодо інформаційної безпеки, Конвенцію про кіберзлочинність.	1				

Враховуючи високий рівень показників, рекомендації щодо Цілі 17 «долучатися до міжнародної співпраці (не тільки з країнами-членами ЄС)» відсутні.