ЄВРОПЕЙСЬКЕ АГЕНТСТВО З ПИТАНЬ МЕРЕЖЕВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

КЕРІВНИЦТВО З ОЦІНКИ НАЦІОНАЛЬНИХ СПРОМОЖНОСТЕЙ

ГРУДЕНЬ 2020

ПРО ЄВРОПЕЙСЬКЕ АГЕНТСТВО З ПИТАНЬ МЕРЕЖЕВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ENISA)

Європейське агентство з питань мережевої та інформаційної безпеки, ENISA, є агентством Європейського Союзу, метою діяльності якого є досягнення високого загального рівня кібербезпеки в Європі. Засноване у 2004 році та у своїй діяльності підкріплене Законом ЄС про кібербезпеку, Європейське агентство з питань мережевої та інформаційної безпеки робить свій внесок у політику ЄС у сфері кібербезпеки, підвищує надійність продуктів, сервісів і процесів ІКТ (інформаційно-комунікаційних технологій) за допомогою схем сертифікації кібербезпеки, співпрацює з країнами-членами та органами ЄС і допомагає Європі підготуватися до кібервикликів майбутнього. Шляхом обміну знаннями, розбудови спроможності та підвищення обізнаності Агентство разом зі своїми ключовими зацікавленими особами працює заради зміцнення довіри до пов'язаної економіки, підвищення стійкості інфраструктури Союзу та, врешті-решт, для забезпечення цифрового захисту європейського суспільства та громадян. Більше інформації на сайті www.enisa.europa.eu.

КОНТАКТНА ІНФОРМАЦІЯ

Для зв'язку з авторами, пишіть, будь ласка, на: resilience@enisa.europa.eu.
Для запитів ЗМІ щодо цього документа, будь ласка, пишіть: press@enisa.europa.eu.

АВТОРИ

Анна Cappi (Anna Sarri), Пінелопі Кірануді (Pinelopi Kyranoudi) — Європейське агентство з питань мережевої та інформаційної безпеки (ENISA)
Од Tippio (Aude Thirriot), Федеріко Кареллі (Federico Charelli), Янг Домінік (Yang Dominique) — компанія "Вейвстоун" (Wavestone)

СЛОВА ВДЯЧНОСТІ

ENISA висловлює подяку та вдячність усім експертам, які взяли участь і надали важливі дані для цього звіту, особливо вдячні (в алфавітному порядку латиницею):

Central State Office for the Development of the Digital Society — Центральний державний офіс з питань розвитку цифрового суспільства (Угорщина), Марін Анте Півчевич (Marin Ante Pivcevic)

Centre for Cyber Security — Центр кібербезпеки (Бельгія)

CFCS — Центр кібербезпеки (Данія), Томас Вульфф (Thomas Wulff)

European Cybercrime Centre — Європейський центр боротьби з кіберзлочинністю (EC3), Альсофра Мартінес Альваро (Alzofra Martinez Alvaro)

European Cybercrime Centre — Європейський центр боротьби з кіберзлочинністю (EC3), Адріан-Іонут Бобейка (Adrian-Ionut Bobeica)

Federal Ministry of the Interior — Федеральне міністерство внутрішніх справ (Німеччина), Саша-Александр Леттґен (Sascha-Alexander Lettgen)

Information Security Administration — Управління інформаційної безпеки (Республіка Словенія), Мар'ян Кавчич (Marjan Kavčič)

Італійський уряд (Італія)

Malta Information Technology Agency — Мальтійське агентство з питань інформаційних технологій (Мальта), Катя Бонелло (Katia Bonello) та Мартін Каммілері (Martin Camilleri)

Ministry of Justice and Public Security — Міністерство юстиції і громадської безпеки (Норвегія), Робін Бакке (Robin Bakke)

Ministry of Digital Policy — Міністерство цифрової політики (Греція), Георге Дрівас (George Drivas), Несторас Чуліарас (Nestoras Chouliaras), Євгенія Цапралі (Evgenia Tsaprali) та Сотірис Васілос (Sotiris Vasilos)

Ministry of Economic Affair and Communication — Міністерство з економічних питань та інфраструктури (Естонія), Анна-Ліса Перналаас (Anna-Liisa Pärnalaas)

National Cyber and Information Security Agency — Національне агентство з питань мережевої та інформаційної безпеки (Республіка Чехія), Вероніка Нетоліцка (Veronika Netolická)

National Security Authority — Агентство національної безпеки (Словаччина)

National Security Department — Департамент національної безпеки (Іспанія), Марія Мар Лопес Хіл (Maria Mar Lopez Gil)

NCTV — Міністерство юстиції та безпеки (Нідерланди)

Portuguese National Cybersecurity Centre — Португальський центр національної кібербезпеки (Португалія), Александре Лейте (Alexandre Leite) та Педро Матус (Pedro Matos)

Cyber Security Policy Division, Department of Environment, Climate and Communications — Відділ кібербезпеки, Міністерство зв'язку, енергетики і природних ресурсів (Ірландія), Джеймс Кефрі (James Caffrey)

Оксфордський університет — Центр глобальних спроможностей кібербезпеки (Global Cyber Security Capacity Centre), Керолін Вайсер Харріс (Carolin Weisser Harris)

ENISA також хотіло б подякувати за цінний внесок у це дослідження всім експертам, які надали інформацію, але бажають залишатися анонімними.

ПРАВОВЕ ПОПЕРЕДЖЕННЯ

Звертаємо увагу, що в цій публікації наведені погляди та пояснення ENISA, якщо не зазначено інше. Ця публікація не повинна трактуватись як правовий акт ENISA або органів ENISA, поки її не буде ухвалено відповідно до Регламенту (ЄС) № 2019/881. Ця публікація не обов'язково представляє сучасний стан справ, і ENISA може час від часу оновлювати її.

Сторонні джерела цитуються належним чином. ENISA не несе відповідальності за зміст зовнішніх джерел, у тому числі зовнішніх вебсайтів, на які є посилання в цій публікації.

Ця публікація призначена лише для інформаційних цілей. Вона повинна бути у безоплатному доступі. Ані ENISA, ані будь-яка особа, яка діє від її імені, не несе відповідальності за можливе використання інформації, що міститься в цій публікації.

ПОВІДОМЛЕННЯ ПРО АВТОРСЬКІ ПРАВА

ISBN: 978-92-9204-443-5

DOI: 10.2824/590072

КАТАЛОГ: TP-06-20-047-EN-N

1. ЗМІСТ

СЛОВНИК ТЕРМІНІВ

СКОРОЧЕННЯ	ВИЗНАЧЕННЯ
ШІ	Штучний інтелект
C2M2	Модель зрілості спроможності кібербезпеки
CCRA	Угода про визнання спільних критеріїв
CCSMM	Модель зрілості кібербезпеки громади
КВІІ	Критично важливо інформаційна інфраструктура
CMM	Модель зрілості спроможностей кібербезпеки для держав
CMMC	Сертифікація моделі зрілості кібербезпеки
CPI	Індекс кіберпотужності
Команда CSIRT	Команда з реагування на інциденти в галузі комп'ютерної безпеки
CVD	Координоване розкриття інформації про вразливість
DPA	Закон про захист інформації
ЄЦР	Єдиний цифровий ринок
ECCG	Європейська група з сертифікації кібербезпеки
ECSM	Європейський місяць кібербезпеки
ECSO	Європейська організація з кібербезпеки
ЄАВТ	Європейська асоціація вільної торгівлі
ЄРК	Європейська рамка кваліфікацій
ЄС	Європейський Союз
GCI	Глобальний індекс кібербезпеки
GDPR	Загальний регламент захисту даних
GDS	Державна служба цифрових послуг
IA-CM	Модель спроможності внутрішнього аудиту державного сектору
ІКТ	Інформаційно-комунікаційні технології
ISMM	Модель зрілості інформаційної безпеки для Керівництва NIST з кібербезпеки
МСЕ	Міжнародний союз електрозв'язку
Правоохоронні органи	Державні органи, що здійснюють правоохоронну діяльність
Країна-член	Країна — член ЄС
NCSS	НАЦІОНАЛЬНІ СТРАТЕГІЇ ЩОДО БЕЗПЕКИ МЕРЕЖЕВИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

NIS	Мережева та інформаційна безпека
NIST	Національний інститут стандартів і технології
Координатори	Національні офіцери з координації
ООП	Оператори основних послуг
ОТ	Операційна технологія
PET	Технології підвищення конфіденційності
СУІБ	Система управління інформаційною безпекою конфіденційних даних
ДПП	Державно-приватне партнерство
Q-C2M2	Катарська модель зрілості спроможності кібербезпеки
НДДКР	Науково-дослідні та дослідно-конструкторські роботи
МСП	Малі та середні підприємства
Група SOG-IS MRA	Група старших офіцерів з питань безпеки інформаційних систем у рамках Угоди про взаємне визнання

КОРОТКИЙ ОГЛЯД

Оскільки поточне середовище кіберзагроз продовжує розширюватися, а інтенсивність та кількість кібератак продовжують збільшуватись, у країн-членів ЄС є необхідність ефективно на них реагувати шляхом подальшого удосконалення й адаптації своїх національних стратегій кібербезпеки. З моменту публікації у 2012 році перших досліджень ENISA, пов'язаних з національними стратегіями кібербезпеки, країни — члени ЄС та країни ЄАВТ досягли значного прогресу в розробці та реалізації своїх стратегій.

У цьому звіті представлена робота, проведена ENISA щодо створення Керівництва з оцінки національних спроможностей (КОНС).

Керівництво націлене на надання країнам-членам самооцінки рівня їх зрілості шляхом оцінки цілей їх Національної стратегії кібербезпеки, що допоможе їм посилити та розбудувати спроможності кібербезпеки як на стратегічному, так і на оперативному рівні.

Вона окреслює простий репрезентативний погляд на рівень зрілості кібербезпеки країни-члена. КОНС — це інструмент, який допомагає країнам-членам:

- надати корисну інформацію для розробки довгострокової стратегії (наприклад, корисний досвід, настанови);
- допомогти визначити відсутні елементи в Нацстратегії кібербезпеки;
- допомогти в подальшій розбудові спроможностей кібербезпеки;
- підтримати підзвітність політичних дій;
- забезпечити довіру до широкої громадськості та міжнародних партнерів;
- підтримати інформаційно-пояснювальну роботу та покращити громадську репутацію й авторитет як прозорої організації;
- допомогти передбачити проблеми, що можуть виникнути в майбутньому;
- допомогти визначити надбаний досвід та передові практики;
- забезпечити базовий рівень спроможності кібербезпеки в ЄС для сприяння дискусіям; а також
- допомогти оцінити національні спроможності щодо кібербезпеки.

Це Керівництво було розроблене за підтримки фахових експертів ENISA з питань кібербезпеки та представників 19 країн-членів та країн ЄАВТ[1]. Цільова аудиторія цього звіту — політики, експерти та державні службовці, відповідальні або залучені до розробки, впровадження та оцінки Національної стратегії кібербезпеки, а також, на більшому рівні, спроможностей кібербезпеки.

[1] Були опитані представники з таких країн-членів та країн ЄАВТ: Бельгії, Хорватії, Чехії, Данії, Естонії, Німеччини, Греції, Угорщини, Ірландії, Італії, Ліхтенштейну, Мальти, Нідерландів, Норвегії, Португалії, Словаччини, Словенії, Іспанії, Швеції.

Керівництво з оцінки національних спроможностей охоплює 17 стратегічних цілей і структуроване навколо чотирьох основних кластерів:

- Кластер № 1: Управління та стандарти кібербезпеки
  1. Розробити план реагування на інциденти кібербезпеки
  2. Встановити базові заходи безпеки
  3. Забезпечити захист цифрової ідентифікації та зміцнення довіри до цифрових державних послуг

- Кластер № 2: Нарощування спроможностей та підвищення обізнаності
  4. Організувати тренування з кібербезпеки
  5. Встановити спроможність реагування на інциденти
  6. Підвищити обізнаність користувачів
  7. Посилити навчальні та освітні програми
  8. Сприяти науково-дослідним і дослідно-конструкторським роботам
  9. Забезпечити стимули для приватного сектору інвестувати в заходи безпеки
  10. Покращити кібербезпеку ланцюга постачання

- Кластер № 3: Нормативно-правова база
  11. Захистити критично важливу інформаційну інфраструктуру, ООП і ПЗО
  12. Займатися протидією кіберзлочинності
  13. Встановити механізми звітування про інциденти
  14. Посилити конфіденційність та захист даних

- Кластер № 4: Співпраця
  15. Встановити державно-приватне партнерство
  16. Надати інституційний характер співпраці між державними органами
  17. Долучатися до міжнародної співпраці

1. ВСТУП

Директива щодо мережевої та інформаційної безпеки (NIS), опублікована в липні 2016 року, вимагає від країн — членів ЄС прийняття національної стратегії з безпеки мережевих та інформаційних систем, яка також називається Національна стратегія кібербезпеки (NCSS), як викладено у статтях 1 та 7. У цьому контексті Національна стратегія кібербезпеки визначається як концептуальна рамка, яка встановлює стратегічні принципи, настанови, стратегічні цілі, пріоритети, відповідні політики та регуляторні заходи. Передбаченою метою Національної стратегії кібербезпеки є досягнення та підтримка високого рівня безпеки мережі та систем, що дозволить країнам-членам зменшувати рівень потенційних загроз. До того ж Національна стратегія кібербезпеки також може бути каталізатором для промислового розвитку та соціально-економічного прогресу.

Закон ЄС про кібербезпеку передбачає, що ENISA сприятиме розповсюдженню передових практик у визначенні та впровадженні Національної стратегії кібербезпеки, надаючи підтримку країнам-членам у впровадженні Директиви NIS та збираючи цінні відгуки про їх досвід. Із цією метою ENISA розробила кілька інструментів для надання допомоги країнам-членам у розробці, впровадженні та оцінці їх національних стратегій кібербезпеки.

У рамках свого мандату ENISA має на меті розробити Керівництво з самооцінки національних спроможностей для вимірювання рівня готовності різних національних стратегій кібербезпеки. Мета цього звіту — представити дослідження, проведене щодо визначення Керівництва з самооцінки.

1.1 СФЕРА ТА ЦІЛІ ДОСЛІДЖЕННЯ

Головною метою цього дослідження є створення Керівництва з самооцінки національних спроможностей, що згодом іменується КОНС, для вимірювання рівня зрілості спроможностей кібербезпеки країн-членів. Більш конкретно Керівництво повинне надати країнам-членам можливість:

- проведення оцінки своїх національних спроможностей кібербезпеки;
- підвищення обізнаності про рівень готовності країни;
- визначення напрямів для вдосконалення; а також
- розбудови спроможностей кібербезпеки.

Це Керівництво повинне допомогти країнам-членам і, зокрема, національним політикам провести тренувальні заходи із самооцінки з метою вдосконалення національних спроможностей кібербезпеки.

1.2 МЕТОДОЛОГІЧНИЙ ПІДХІД

Методологічний підхід, що використовується для розробки Керівництва з самооцінки національних спроможностей, спирається на чотири основні кроки.

1. **Кабінетне дослідження**. Першим кроком було проведення широкого огляду літератури для збору передових практик щодо розробки керівництва з оцінки зрілості для національних стратегій кібербезпеки. Кабінетне дослідження сфокусоване на систематичному аналізі відповідних документів щодо розбудови спроможності кібербезпеки та визначення стратегії, на наявних національних стратегіях кібербезпеки країн-членів і на порівнянні наявних моделей зрілості щодо кібербезпеки. Контрольне випробування на наявних моделях зрілості проведене шляхом застосування керівництва для аналізу, розробленого для цілей цього дослідження.

Керівництво для аналізу спирається на методологію Беккера[2] для розробки моделей зрілості, яка встановлює загальну та консолідовану модель порядку проєктування моделей зрілості та забезпечує чіткі вимоги до розробки моделей зрілості. Потім керівництво для аналізу було додатково налаштоване для задоволення потреб цього дослідження.

2. **Збір думок експертів та зацікавлених осіб.** На основі даних, зібраних за допомогою кабінетного дослідження, і пов'язаних попередніх висновків аналізу цей етап передбачав визначення та запрошення на співбесіду визначених експертів, які мають досвід у розробці та впровадженні національних стратегій кібербезпеки або моделей зрілості. ENISA зв'язалася зі своєю групою експертів з питань національних стратегій кібербезпеки та національними офіцерами з координації (координаторами), аби знайти відповідних експертів у кожній країні-члені. Крім того, було проведено співбесіду з деякими експертами, які брали участь у розробці моделей зрілості. Загалом було проведено 22 співбесіди, 19 з яких проходили з представниками агентств з питань кібербезпеки в різних країнах-членах (та країнах ЄАВТ).

3. **Аналіз накопичених вхідних даних.** Дані, зібрані в процесі кабінетного дослідження та під час співбесід, згодом були проаналізовані для виявлення передових практик у розробці керівництва з самооцінки для вимірювання зрілості Національної стратегії кібербезпеки, для розуміння потреб країн-членів та визначення даних, які можна зібрати в різних європейських країнах[3]. Цей аналіз дозволив доопрацювати попередню модель, розроблену на попередніх кроках, та уточнити набір показників, що входять до моделі, рівні зрілості та її виміри.

4. **Завершення моделі.** Після цього оновлена версія керівництва з самооцінки національних спроможностей була проаналізована експертами ENISA, які є фахівцями в цій галузі, а потім додатково затверджена експертами на семінарі-практикумі, проведеному в жовтні 2020 р. перед публікацією.

1.3 ЦІЛЬОВА АУДИТОРІЯ

Цільова аудиторія цього звіту — це політики, експерти та державні службовці, відповідальні або залучені до розробки, впровадження та оцінки Національної стратегії кібербезпеки, а також, на більшому рівні, спроможностей кібербезпеки. Крім того, формалізовані в цьому документі висновки можуть бути цінними для експертів та дослідників з питань політики кібербезпеки на національному та європейському рівнях.

[2] J. Becker, R. Knackstedt, and J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application," Business & Information Systems Engineering, vol. 1, no. 3, pp. 213–222, Jun. 2009.
[3] Для цілей цього дослідження термін "європейські країни", який згадується у цьому звіті, включає 27 країн — членів ЄС.

2. ПЕРЕДУМОВИ

2.1 ПОПЕРЕДНЯ РОБОТА ЩОДО ЖИТТЄВОГО ЦИКЛУ НАЦІОНАЛЬНИХ СТРАТЕГІЙ КІБЕРБЕЗПЕКИ

Як зазначено в Законі ЄС про кібербезпеку, однією з головних цілей ENISA є підтримка країн-членів у розробці національних стратегій щодо безпеки мережевих та інформаційних систем, сприяння розповсюдженню цих стратегій і контроль за їх виконанням. У рамках свого мандату ENISA підготувало кілька документів на цю тему, аби сприяти обміну корисним досвідом та підтримати впровадження Національних стратегій кібербезпеки в ЄС:

- "Практичний посібник з етапу розробки та виконання Національної стратегії кібербезпеки"[4], опублікований 2012 року;
- "Встановлення курсу національних зусиль щодо зміцнення безпеки в кіберпросторі"[5], опубліковане 2012 року;
- Перше керівництво ENISA для оцінювання національних стратегій кібербезпеки країни-члена, опубліковане[6] 2014 року;
- "Інтерактивна онлайн мапа Національної стратегії кібербезпеки"[7], опублікована 2014 року;
- "Керівництво з належної практики впровадження Національної стратегії кібербезпеки"[8], опубліковане 2016 року;
- "Інструмент оцінки національної стратегії кібербезпеки"[9], опубліковане 2018 року;
- "Корисний досвід інноваційної діяльності в галузі кібербезпеки в рамках Національної стратегії кібербезпеки"[10], опубліковане 2019 року.

ДОДАТОК А містить короткий огляд основних публікацій ENISA з цієї теми.

Вищезазначені посібники та документи були досліджені в рамках кабінетного дослідження. Зокрема, "Інструмент оцінки національної стратегії кібербезпеки" [11] є базовим елементом КОНС. КОНС ґрунтується на цілях, окреслених в інтернет-інструменті оцінки Національної стратегії кібербезпеки.

2.2 СПІЛЬНІ ЦІЛІ, ВИЗНАЧЕНІ В НАЦІОНАЛЬНИХ СТРАТЕГІЯХ ЄС ЩОДО БЕЗПЕКИ МЕРЕЖЕВИХ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Відмінності між різними країнами-членами ускладнюють визначення спільних заходів або планів дій між різними національними особливостями, правовими системами та політичними програмами.

---

[4] Національна стратегія кібербезпеки: практичний посібник з розробки та виконання (ENISA, 2012)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] Національна стратегія кібербезпеки: встановлення курсу національних зусиль щодо зміцнення безпеки в кіберпросторі (ENISA, 2012)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] Керівництво з оцінювання для Національної стратегії кібербезпеки (ENISA, 2014)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] Національні стратегії кібербезпеки — інтерактивна мапа (ENISA, 2014, оновлено у 2019 році)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Цей документ вносить правки до посібника за 2012 рік: Керівництво з належної практики впровадження Національної стратегії кібербезпеки: розробка та впровадження національних стратегій кібербезпеки (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] Інструмент оцінки національної стратегії кібербезпеки (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] Інструмент оцінки національної стратегії кібербезпеки (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

Однак національні стратегії кібербезпеки країн-членів часто містять стратегічні цілі, сформульовані стосовно тих самих тем. Таким чином, на основі попередньої роботи ENISA та аналізу національних стратегій кібербезпеки країн-членів було визначено 22 стратегічні цілі. 15 із цих стратегічних цілей вже були визначені в попередній роботі ENISA, 2 були нещодавно додані в цьому дослідженні та 5 цілей були визначені для подальших розглядів.

2.2.1 Спільні стратегічні цілі, які зазначені країнами-членами

На основі попередньої роботи ENISA, а саме на основі інструменту оцінки Національної стратегії кібербезпеки[12], у поданій нижче таблиці наведено вищезгаданий набір з 15 стратегічних цілей, які спільно охоплені національними стратегіями кібербезпеки країн-членів. Цілі окреслюють суть загальної "національної філософії" з цієї теми. Для отримання додаткової інформації про цілі, описані нижче, зверніться до звіту ENISA "Керівництво з належної практики впровадження Національної стратегії кібербезпеки"[13].

Таблиця 1. Спільні стратегічні цілі, визначені країнами-членами у своїх національних стратегіях щодо безпеки мережевих та інформаційних систем

Ід. №	Стратегічні цілі національних стратегій кібербезпеки	Цілі
1	**Розробити національні плани реагування на інциденти кібербезпеки**	► Представити та пояснити критерії, якими слід використовувати для визначення ситуації як кризи ► Визначити ключові процеси та дії для обробки кризових ситуацій ► Чітко визначити функції та відповідальність різних зацікавлених осіб під час кіберкризи ► Представити та пояснити критерії виходу з кризи та/або хто має повноваження оголосити про це
2	**Встановити базові заходи безпеки**	► Гармонізувати різні практики дій, яких дотримуються організації як у державному, так і в приватному секторі ► Створити спільну мову між компетентними державними органами та організаціями та відкрити захищені канали зв'язку ► Надати можливість різним зацікавленим особам перевіряти та оцінити ефективність своїх спроможностей кібербезпеки ► Ділитися інформацією про корисний досвід у сфері кібербезпеки в кожній галузі ► Допомогти зацікавленим особам визначити пріоритет стосовно своїх інвестицій у безпеку
3	**Організувати тренування з кібербезпеки**	► Визначити, що потрібно протестувати (плани та процеси, люди, інфраструктура, спроможності реагування, спроможності співпраці, комунікація тощо) ► Створити національну групу з планування тренувань з кібербезпеки, наділивши її чітким мандатом ► Інтегрувати тренування з кібербезпеки у життєвий цикл національної стратегії кібербезпеки або національний план реагування на інциденти кібербезпеки.
4	**Встановити спроможність реагування на інциденти**	► Мандат стосується повноважень, функцій і відповідальності, якими відповідний уряд повинен наділити команду ► Портфель сервісів охоплює сервіси, які команда надає своїм клієнтам або використовує для власного внутрішнього функціонування ► Експлуатаційні спроможності стосуються технічних та експлуатаційних вимог, яких повинна дотримуватися команда ► Спроможності співпраці включають вимоги щодо обміну інформацією з іншими командами, які не охоплені попередніми трьома категоріями, наприклад, політиками, військовими, регуляторами, операторами (критично важливої інформаційної інфраструктури), правоохоронними органами.

[12] Інструмент оцінки національної стратегії кібербезпеки (2018)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

[13] Цей документ вносить правки до посібника за 2012 рік: Керівництво з належної практики впровадження Національної стратегії кібербезпеки: розробка та впровадження національних стратегій кібербезпеки (ENISA, 2016)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Ід. №	Стратегічні цілі національних стратегій кібербезпеки	Цілі
5	**Підвищити обізнаність користувачів**	► Виявити прогалини у знаннях, що стосуються кібербезпеки чи питань інформаційної безпеки ► Усунути прогалини шляхом підвищення обізнаності або розвитку/зміцнення базових знань
6	**Посилити навчальні та освітні програми**	► Посилити експлуатаційні спроможності наявного персоналу з питань інформаційної безпеки ► Заохочувати студентів приєднуватися, а потім готувати їх до входження у сферу кібербезпеки ► Сприяти та заохочувати стосунки між академічними колами у сфері інформаційної безпеки та галуззю інформаційної безпеки ► Узгодити програми підготовки з кібербезпеки з потребами бізнесу
7	**Сприяти науково-дослідним і дослідно-конструкторським роботам**	► Визначити справжні причини вразливостей, замість того, аби усувати їх вплив ► Об'єднати вчених з різних дисциплін для вирішення багатовимірних і складних проблем, таких як фізичні кіберзагрози ► Об'єднати потреби промисловості та результати досліджень, полегшуючи тим самим перехід від теорії до практики; ► Знайти способи не лише підтримувати, але й підвищувати рівень кібербезпеки продуктів і сервісів, що підтримують наявні інфраструктури кібербезпеки
8	**Забезпечити стимули для приватного сектору інвестувати в заходи безпеки**	► Визначити можливі стимули для приватних компаній інвестувати в заходи безпеки ► Надавати компаніям стимули для заохочення інвестицій у безпеку
9	**Захистити критично важливу інформаційну інфраструктуру, ООП і ПЗО (КВІІ)**	► Визначити критично важливу інформаційну інфраструктуру ► Виявити та зменшити вплив відповідних ризиків для кластера КВІІ
10	**Займатися протидією кіберзлочинності**	► Створення законів у галузі кіберзлочинності ► Підвищення ефективності діяльності правоохоронних органів
11	**Встановити механізми звітування про інциденти**	► Отримати знання про загальне середовище загроз ► Оцінити вплив інцидентів (наприклад, порушення безпеки, збої в роботі мережі, перебої в роботі систем) ► Отримати знання про наявні та нові вразливості та типи атак ► Відповідно оновити заходи безпеки ► Впровадити положення Директиви NIS щодо звітування про події
12	**Посилити конфіденційність та захист даних**	► Сприяти посиленню основних прав щодо конфіденційності та захисту даних
12	**Встановити державно-приватне партнерство (ДПП)**	► Стримування (стримувати дії зловмисників) ► Захист (використовує дослідження для нових загроз безпеці) ► Виявлення (використовує обмін інформацією для вирішення нових загроз) ► Реагування (надання спроможності реагувати при початковому впливі інциденту) ► Відновлення (надання спроможності відновлення після закінчення впливу інциденту)
14	**Надати інституційний характер співпраці між державними органами**	► Посилити співпрацю між державними установами, які відповідають та мають компетенцію у сфері кібербезпеки ► Уникати дублювання компетенції та ресурсів між державними установами ► Поліпшити та надати інституційний характер співпраці між державними установами в різних сферах кібербезпеки.
15	**Долучатися до міжнародної співпраці (не тільки з країнами — членами ЄС)**	► Отримати користь від створення спільної бази знань між країнами — членами ЄС ► Створити ефекти синергії між національними органами кібербезпеки ► Зробити можливою та посилити боротьбу з транснаціональною злочинністю

2.2.2 Додаткові стратегічні цілі

На основі виконаного кабінетного дослідження та співбесід, проведених ENISA, були визначені додаткові стратегічні цілі. Країни-члени дедалі частіше звертаються до цих тем у своїх національних стратегіях кібербезпеки або визначають свої плани дій, базуючись на тому самому предметі. Також наводяться приклади діяльності країн-членів. Якщо приклад наводиться із загальнодоступного джерела, надається посилання. У випадках, коли приклади базуються на конфіденційних співбесідах з посадовими особами країн — членів ЄС, посилання не надаються.

Були визначені такі додаткові стратегічні цілі:

- покращити кібербезпеку ланцюга постачання і
- забезпечити захист цифрової ідентифікації та зміцнення довіри до цифрових державних послуг.

Покращити кібербезпеку ланцюга постачання

Малі та середні підприємства (МСП) є основою європейської економіки. Вони представляють 99 % усіх суб'єктів господарювання в ЄС[14], а 2015 року було підраховано, що МСП створили близько 85 % нових робочих місць і забезпечили дві третини загальної зайнятості приватного сектору в ЄС. Крім того, оскільки МСП надають послуги великим компаніям і дедалі більше працюють з державними адміністративними органами[15], необхідно зазначити, що в сучасній взаємопов'язаній дійсності МСП є слабкою ланкою для кібератак. Дійсно, МСП є найбільш схильними до кібератак, проте вони часто не можуть дозволити собі адекватно інвестувати в кібербезпеку[16]. Таким чином, поліпшення кібербезпеки ланцюга постачання повинно здійснюватися з акцентом на МСП.

На додаток до цього системного підходу країни-члени можуть також зробити наголос на зусиллях щодо кібербезпеки певних сервісів і продуктів ІКТ, які вважаються необхідними: ІКТ-технології, що використовуються в критично важливій інформаційній інфраструктурі, механізми безпеки, що обов'язково застосовуються в телекомунікаційному секторі (контроль на рівні інтернет-провайдера тощо), довірчі послуги, як визначено в регламенті eIDAS, та постачальники хмарних сервісів. Наприклад, у своїй національній стратегії кібербезпеки на 2019—2024 роки[17] Польща взяла на себе зобов'язання розробити національну систему оцінки та сертифікації кібербезпеки як механізм забезпечення якості в ланцюгу постачання. Ця система сертифікації буде узгоджена з Керівництвом ЄС з сертифікації цифрових продуктів, сервісів і процесів ІКТ, визначеним Законом ЄС про кібербезпеку (2019/881).

Таким чином, покращення кібербезпеки ланцюга постачання має першорядне значення. Цього можна досягти шляхом встановлення суворої політики сприяння МСП, надання настанов щодо вимог до кібербезпеки в процедурах закупівель у сфері державного управління, сприяння співпраці в приватному секторі, розбудови ДПП, сприяння механізмам координованого розкриття інформації про вразливість (CVD)[18], побудові схеми сертифікації продуктів, у тому числі, серед іншого, компонентів кібербезпеки в цифрових ініціативах для МСП та фінансування, розвитку навичок.

Забезпечити захист цифрової ідентифікації та зміцнення довіри до цифрових державних послуг

У лютому 2020 року Комісія виклала своє бачення цифрової трансформації ЄС у повідомленні «Формування цифрового майбутнього Європи»[19] з метою донесення інклюзивних технологій, які працюють для людей та поважають фундаментальні цінності ЄС. Зокрема, у повідомленні зазначається, що сприяння цифровій трансформації державних адміністративних органів у всій Європі є вкрай важливим. У цьому сенсі формування довіри до уряду щодо цифрової ідентифікації та довіри до державних послуг має першорядне значення.

---

[14] https://ec.europa.eu/growth/smes/
[15] https://www.oecd.org/fr/publications/smes-in-public-procurement-9789264307476-en.htm
[16] https://www.eesc.europa.eu/en/news-media/news/european-companies-especially-smes-face-growing-risk-cyber-attacks-study
[17] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[18] https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
[19] Формування цифрового майбутнього Європи, COM(2020) 67 кінцевий варіант: https://ec.europa.eu/info/sites/info/files/communication-shaping-europes-digital-future-feb2020_en_3.pdf

Це ще більш критично важливо, якщо врахувати той факт, що трансакції в державному секторі та обмін даними часто мають секретний характер.

Багато країн висловили свої наміри розглянути цю тему у своїх національних стратегіях кібербезпеки, зокрема: Данія, Естонія, Франція, Люксембург, Мальта, Іспанія, Нідерланди та Великобританія. Серед цих країн деякі також заявили, що ця стратегічна ціль може бути розглянута як частина більш загального плану.

- Естонія пов'язує свій спільний план дій "Безпека електронної ідентифікації та спроможності електронної автентифікації" із більш загальною Цифровою програмою на 2020 рік для Естонії.
- Французька національна стратегія кібербезпеки вказує, що державний секретар, відповідальний за цифрові технології, контролює створення дорожньої карти "для захисту цифрового життя, конфіденційності та персональних даних французів".
- Нідерландська національна стратегія кібербезпеки стверджує, що кібербезпека в державних адміністративних органах, а також державні послуги, що надаються громадянам та бізнесу, детальніше розкриваються в "Широкій програмі дій для цифрового уряду".
- Оскільки уряд Великобританії продовжує розміщувати більшу частину своїх сервісів в Інтернеті, він призначив Державну службу цифрових сервісів (GDS), аби гарантувати, що всі нові цифрові сервіси, розроблені або закуплені урядом, також були "безпечними за налаштуванням", за підтримки Британського національного центру кібербезпеки (NCSC).

2.2.3 інші розглянуті стратегічні цілі

На етапі проведення кабінетного дослідження та в рамках співбесід, проведених ENISA, досліджувалися інші стратегічні цілі. Однак було вирішено, що ці цілі не стануть частиною керівництва з самооцінки. ДОДАТОК C — Інші досліджувані цілі містять визначення кожної з цих цілей, які можуть бути використані для надання поштовху подальшим обговоренням щодо можливих удосконалень національних стратегій кібербезпеки.

Зазначені нижче стратегічні цілі були вивчені як наступні теми для розгляду:

- розробити галузеві стратегії кібербезпеки,
- боротися з кампаніями дезінформації,
- забезпечити використання передових технологій (5G, ШІ, обчислення за допомогою квантових комп'ютерів тощо);
- забезпечити суверенітет даних; а також
- забезпечити стимули для розвитку галузі кіберстрахування.

2.3 ОСНОВНІ РЕЗУЛЬТАТИ І ВИСНОВКИ КОНТРОЛЬНОГО ВИПРОБУВАННЯ

Кабінетне дослідження наявних моделей зрілості, пов'язаних з кібербезпекою, було проведене з метою збору інформації та доказів на підтримку створення проєкту керівництва з самооцінки національних спроможностей у сфері дії Національної стратегії кібербезпеки. У цьому контексті було проведено розлогий аналіз літератури щодо наявних моделей, аби доповнити висновки первинного масштабного дослідження моделей зрілості кібербезпеки та наявних національних стратегій кібербезпеки, розроблених у розділах 2.1 та 2.2. Цей систематичний огляд підтримує вибір та обґрунтування рівнів зрілості керівництва з оцінки та визначення різних вимірів і показників.

У рамках систематичного аналізу моделей зрілості було розглянуто та проаналізовано 10 моделей на основі їх ключових особливостей. Глобальний огляд ключових особливостей кожної моделі, проаналізованої в рамках цього дослідження, поданий у таблиці 2 "Огляд аналізованих **моделей** зрілості", а більш детальний аналіз можна знайти в ДОДАТКУ A.

Таблиця 2. Огляд проаналізованих моделей зрілості

Назва моделі	Кількість рівнів зрілості	Кількість атрибутів	Метод оцінки	Представлення результатів
Модель зрілості спроможностей кібербезпеки для держав (CMM)	5	5 основних вимірів	Співпраця з місцевою організацією з метою доопрацювання моделі перед її застосуванням в національному контексті	5-секційний радар
Модель зрілості спроможностей кібербезпеки (C2M2)	4	10 основних сфер	Методологія та набір інструментів для самооцінювання	Таблиця показників із секторними діаграмами
Керівництво для удосконалення кібербезпеки критично важливої інфраструктури	немає даних (4 яруси)	5 основних функцій	Самооцінка	немає даних
Катарська модель зрілості спроможностей кібербезпеки (Q-C2M2)	5	5 основних сфер	немає даних	немає даних
Сертифікація моделі зрілості кібербезпеки (CMMC)	5	17 основних сфер	Оцінка сторонніми аудиторами	немає даних
Модель зрілості кібербезпеки громади (CCSMM)	5	6 основних вимірів	Оцінка в громадах на основі даних, отриманих від державних і федеральних правоохоронних органів	немає даних
Модель зрілості інформаційної безпеки для Керівництва NIST з кібербезпеки (ISMM)	5	23 оцінені сфери	немає даних	немає даних
Модель спроможності внутрішнього аудиту (IA-CM) для державного сектору	5	6 елементів	Самооцінка	немає даних
Глобальний індекс кібербезпеки (GCI)	НЕМАЄ ДАНИХ	5 стовпів	Самооцінка	Рейтингова таблиця
Індекс кіберпотужності (CPI)	НЕМАЄ ДАНИХ	4 категорії	Оцінка ефективності, проведена компанією "Економіст Інтеліджене Юніт"	Рейтингова таблиця

Цей систематичний аналіз дозволив зробити висновки щодо передових практик, прийнятих у наявних моделях, з метою підтримки розробки концептуальної моделі для поточної моделі зрілості. Зокрема, проведене контрольне випробування підтримало визначення рівнів зрілості, створення кластерів вимірів і вибір показників, а також відповідну методологію візуалізації результатів моделі. Найбільш відповідні висновки щодо кожного з цих елементів детально описані в таблиці 3.

Таблиця 3. Основні результати та висновки контрольного випробування

Характеристика	Ключовий висновок
Рівні зрілості	► Загальновизнаною є п'ятирівнева шкала зрілості для керівництв з оцінки спроможностей кібербезпеки, яка може надати детальні результати оцінки (див. таблицю 6 «Порівняння рівнів зрілості для вичерпного уявлення про визначення рівнів зрілості для кожної моделі»). ► Усі моделі забезпечують високий рівень визначення кожного рівня зрілості, який потім адаптується до різних вимірів або кластерів вимірів. ► Зазвичай під час вимірювання зрілості спроможностей кібербезпеки оцінюються два основні аспекти: зрілість стратегій та зрілість процесів, запроваджених для реалізації стратегій.
Атрибути	► Порівняльний аналіз атрибутів наявних моделей зрілості показує неоднорідні результати із середньою кількістю атрибутів на модель від чотирьох до п'яти. ► Модель, що спирається приблизно на чотири або п'ять атрибутів, забезпечує країнам правильний рівень деталізації даних, групуючи відповідні виміри разом та забезпечуючи читабельність результатів (див. таблицю 7« Порівняння атрибутів/**вимірів** для опису атрибутів для кожної моделі»). ► Ключовий принцип, прийнятий усіма моделями при визначенні кластерів, базується на узгодженості елементів, згрупованих у кожному кластері.
Метод оцінки	► Методи оцінки, що використовуються в різних аналізованих моделях, різняться один від одного. ► Найпоширеніший метод оцінки заснований на самооцінці.
Представлення результатів	► Важливо представляти результати на різному рівні деталізації. ► Методологія візуалізації повинна бути зрозумілою і легкою для сприйняття.

Концептуальна модель була побудована на основі контрольного випробування різних моделей зрілості, а також на попередній роботі, проведеній ENISA. Крім того, було вирішено спиратися на *інтерактивний онлайн-інструмент ENISA* для розробки показників зрілості, що використовуються для кожного атрибута.

2.4 ВИКЛИКИ ЩОДО ОЦІНКИ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ

Країни-члени стикаються з багатьма викликами в процесі розбудови спроможностей кібербезпеки, а точніше, при забезпеченні того, аби їх спроможності враховували останні розробки. Нижче наведено короткий опис викликів, визначених та обговорених з країнами-членами в рамках цього дослідження.

- **Труднощі координації та співпраці:** координація зусиль з кібербезпеки на національному рівні з метою ефективної реакції на проблеми кібербезпеки може виявитися проблемою через велику кількість залучених зацікавлених осіб.
- **Нестача ресурсів для проведення оцінки:** залежно від місцевого контексту та структури управління національною кібербезпекою оцінка Національної стратегії кібербезпеки та її цілей може зайняти понад 15 людино-днів.
- **Нестача підтримки для розвитку спроможностей кібербезпеки:** деякі країни-члени повідомили, що для захисту бюджету та отримання підтримки для розвитку спроможностей кібербезпеки спочатку вони повинні провести етап оцінки для виявлення прогалин та обмежень.
- **Труднощі з віднесенням успіхів або змін до стратегії:** оскільки загрози розвиваються щодня, а технології вдосконалюються, плани дій постійно потребують адаптації у відповідь на ці зміни. Однак оцінювання Національної стратегії кібербезпеки та віднесення змін до самої стратегії залишається важким завданням. Це, зі свого боку, ускладнює виявлення обмежень та недоліків Національної стратегії кібербезпеки.

- **Труднощі з вимірюванням ефективності Національної стратегії кібербезпеки:** метрики можна збирати для вимірювання різних сфер, таких як прогрес, впровадження, зрілість та ефективність. Тоді як вимірювання прогресу та впровадження є досить легким порівняно з вимірюванням ефективності, останнє залишається більш значущим для оцінювання результатів і факторів впливу Національної стратегії кібербезпеки. На підставі співбесід, проведених ENISA, велика кількість країн-членів заявила, що кількісне вимірювання ефективності Національної стратегії кібербезпеки є важливим, але це також являє собою надскладне завдання, яке в деяких випадках є цілком неможливим.
- **Складність прийняття спільного керівництва:** країни — члени ЄС діють у різних контекстах з погляду політики, організацій, культури, структури суспільства та зрілості національних стратегій кібербезпеки. Деякі країни-члени, опитані в рамках цього дослідження, висловили думку, що може бути важко захищати та використовувати єдине "узагальнене" керівництво з самооцінки.

2.5 ПЕРЕВАГИ ОЦІНКИ НАЦІОНАЛЬНИХ СПРОМОЖНОСТЕЙ

З 2017 року всі країни — члени ЄС мають Національну стратегію кібербезпеки[20]. Хоча це і позитивний розвиток, важливо також, аби країни-члени мали змогу належним чином оцінювати такі національні стратегії кібербезпеки, тим самим вносячи додаткову вартість до їх стратегічного планування та впровадження.

Однією з цілей керівництва з оцінки національних спроможностей є оцінка спроможностей кібербезпеки на основі пріоритетів, викладених у різних національних стратегіях кібербезпеки. По суті, керівництво оцінює рівень зрілості спроможностей кібербезпеки країн-членів у сферах, визначених цілями національних стратегій кібербезпеки. Таким чином, результати цього керівництва підтримують політиків країн-членів у визначенні національної стратегії з кібербезпеки, надаючи їм розвідувальну інформацію про стан справ у країні[21]. Зрештою, КОНС має допомогти країнам-членам визначити сфери вдосконалення та розбудови спроможностей.

Керівництво націлене на надання країнам-членам самооцінки рівня їх зрілості шляхом оцінки цілей їх Національної стратегії кібербезпеки, що допоможе їм посилити та розбудувати спроможності кібербезпеки як на стратегічному, так і на оперативному рівні.

На основі більш практичного підходу, що ґрунтується на співбесідах, проведених ENISA з кількома агентствами, відповідальними за сферу кібербезпеки в різних країнах-членах, були визначені та акцентовані такі переваги керівництва з оцінки національних спроможностей:

- надати корисну інформацію для розробки довгострокової стратегії (наприклад, корисний досвід, настанови);
- допомогти визначити відсутні елементи в Нацстратегії кібербезпеки;
- допомогти в подальшій розбудові спроможностей кібербезпеки;
- підтримати підзвітність політичних дій;
- забезпечити довіру до широкої громадськості та міжнародних партнерів;
- підтримати інформаційно-пояснювальну роботу та покращити громадську репутацію й авторитет як прозорої організації;
- допомогти передбачити проблеми, що можуть виникнути в майбутньому;
- допомогти визначити надбаний досвід та передові практики;
- забезпечити базовий рівень спроможності кібербезпеки в ЄС для сприяння дискусіям; а також
- допомогти оцінити національні спроможності щодо кібербезпеки.

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999). The interface between evaluation and public policy. Evaluation, 5(4), 468-486.

3. МЕТОДОЛОГІЯ КЕРІВНИЦТВА З ОЦІНКИ НАЦІОНАЛЬНИХ СПРОМОЖНОСТЕЙ

3.1 ЗАГАЛЬНА МЕТА

Основною метою КОНС є вимірювання рівня зрілості спроможностей кібербезпеки **країн-членів**, аби підтримати їх у проведенні оцінювання їх спроможності національної кібербезпеки, підвищенні обізнаності про рівень зрілості країни, визначенні напрямів для вдосконалення та розбудови спроможностей кібербезпеки.

3.2 РІВНІ ЗРІЛОСТІ

Керівництво базується на **п'яти рівнях зрілості**, що визначають етапи, через які країни-члени проходять під час розбудови спроможностей кібербезпеки у сфері, охопленій кожною метою Національної стратегії кібербезпеки. Ці рівні являють собою висхідні рівні зрілості, починаючи з початкового **рівня 1**, коли країни-члени не мають чітко визначеного підходу до нарощування спроможностей кібербезпеки у сферах, охоплених цілями Національної стратегії кібербезпеки, і закінчуючи **рівнем 5**, коли стратегія з нарощування спроможностей кібербезпеки є динамічною та адаптивною до розвитку навколишнього середовища. У таблиці 4 наведена шкала рівня зрілості з описом кожного рівня зрілості.

Таблиця 4. П'ятирівнева шкала ENISA зрілості Керівництва з оцінки національних спроможностей

РІВЕНЬ 1 — ПОЧАТКОВИЙ/AD HOC	РІВЕНЬ 2 — РАННЄ ВИЗНАЧЕННЯ	РІВЕНЬ 3 — ВСТАНОВЛЕННЯ	РІВЕНЬ 4 — ОПТИМІЗАЦІЯ	РІВЕНЬ 5 — САМОПРИСТОСОВНІСТЬ
Країна-член не має чітко визначеного підходу до розбудови спроможностей кібербезпеки у сферах, охоплених цілями Національної стратегії кібербезпеки. Проте країна могла б уже мати певні загальні цілі та виконала деякі дослідження (технічні, політичні, в рамках політики) для вдосконалення національних спроможностей.	Визначено національний підхід до розбудови спроможностей у сфері, охопленій цілями Національної стратегії кібербезпеки. Наявні плани дій або заходи щодо досягнення результатів, але вони перебувають на ранній стадії. Крім того, могли бути визначені та/або залучені активні зацікавлені сторони.	План дій щодо розбудови спроможностей у сфері, охопленій цілями Національної стратегії кібербезпеки, чітко визначений і підтримується відповідними зацікавленими сторонами. Практика і дії запроваджуються та реалізуються на національному рівні однаково. Визначена та задокументована діяльність з чітким розподілом ресурсів та управлінням, а також зі встановленими строками.	План дій регулярно оцінюється: він стійкий, пріоритетний та оптимізований. Регулярно вимірюється ефективність діяльності з розбудови спроможностей кібербезпеки. Визначені фактори успіху, виклики та прогалини у вчиненні діяльності.	Стратегія з розбудови спроможностей кібербезпеки є динамічною й адаптивною. Постійна увага до екологічно сталого розвитку (технологічні досягнення, глобальний конфлікт, нові загрози тощо) сприяє спроможності швидко приймати рішення та здатності швидко діяти для вдосконалення.

3.3 КЛАСТЕРИ ТА ВСЕОСЯЖНА СТРУКТУРА КЕРІВНИЦТВА З САМООЦІНКИ

Керівництво з самооцінки характеризується **чотирма кластерами**: (I) управління та стандарти кібербезпеки, (II) нарощування спроможностей та підвищення обізнаності, (III) нормативно-правова база та (IV) співпраця. Кожен із цих кластерів охоплює ключову тематичну сферу для розбудови спроможностей кібербезпеки в країні та містить пул різних цілей, які країни-члени можуть включити у свої Національні стратегії кібербезпеки. Зокрема:

- **(I) управління та стандарти кібербезпеки**: цей кластер вимірює спроможність країн-членів встановлювати належне управління, стандарти та корисний досвід у сфері кібербезпеки. Цей вимір враховує різні аспекти кіберзахисту та стійкості, підтримуючи розвиток національної галузі кібербезпеки та зміцнюючи довіру до урядів;
- **(II) нарощування спроможностей та підвищення обізнаності**: цей кластер оцінює спроможність країн-членів підвищувати обізнаність про ризики та загрози кібербезпеки та про способи боротьби з ними. Крім того, цей вимір виявляє здатність країни постійно нарощувати спроможності кібербезпеки та підвищувати загальний рівень знань і навичок у цій галузі. Він розглядає розвиток ринку кібербезпеки та досягнення в галузі НДДКР**.** Цей кластер перегрупує всі цілі, закладаючи основи для сприяння розбудові спроможностей;
- **(III) нормативно-правова база**: цей кластер вимірює спроможність країн-членів запровадити необхідні правові та регуляторні інструменти для врахування та протидії зростанню кіберзлочинності та пов'язаних інцидентів з кібербезпекою, а також для захисту критично важливої інформаційної інфраструктури. Крім того, цей вимір оцінює також спроможність країн-членів створити правову базу для захисту громадян та бізнесу як, наприклад, у випадку з досягненням балансу безпеки та конфіденційності; і
- **(IV) співпраця:** цей кластер оцінює співпрацю та обмін інформацією між різними групами зацікавлених осіб на національному та міжнародному рівнях як важливий інструмент для кращого розуміння та реагування на постійно мінливе середовище загроз.

Цілі, які були включені в модель, є тими, які зазвичай приймаються країнами-членами, і вони були обрані серед цілей, перелічених у розділі 2.2. Зокрема, модель оцінює такі цілі:

- 1. Розробити національні плани реагування на інциденти кібербезпеки (I)
- 2. Встановити базові заходи безпеки (I)
- 3. Забезпечити захист цифрової ідентифікації та зміцнення довіри до цифрових державних послуг (I)
- 4. Встановити спроможність реагування на інциденти (II)
- 5. Підвищити обізнаність користувача (II)
- 6. Організувати тренування з кібербезпеки (II)
- 7. Посилити навчальні та освітні програми (II)
- 8. Сприяти науково-дослідним і дослідно-конструкторським роботам (II)
- 9. Забезпечити стимули для приватного сектору інвестувати в заходи безпеки (II)
- 10. Покращити кібербезпеку ланцюга постачання (II)
- 11. Захист критично важливої інформаційної інфраструктури, ООП і ПЗО (III)
- 12. Займатися протидією кіберзлочинності (III)
- 13. Встановити механізми звітування про інциденти (III)
- 14. Посилити захист конфіденційності даних (III)
- 15. Надати інституційний характер співпраці між державними органами (IV)
- 16. Долучатися до міжнародної співпраці (IV)
- 17. Встановити державно-приватне партнерство (IV)

Чотири кластери та основні цілі поєднані у моделі з метою представлення цілісного уявлення про зрілість спроможностей кібербезпеки країн-членів. На рисунку 1 представлена всеосяжна структура керівництва з самооцінки та показано, як ці елементи, а саме цілі, кластери та керівництво з самооцінки, пов'язані з оцінюванням функціонування країни.

Рисунок 1. Структура керівництва з самооцінки

Для кожної цілі, включеної в керівництво з самооцінки, існує ряд показників, розподілених між п'ятьма рівнями зрілості. Кожен показник базується на дихотомічному запитанні (так чи ні). Показник може бути необхідним або необов'язковим.

3.4 МЕХАНІЗМ НАРАХУВАННЯ БАЛІВ

Механізм нарахування балів для керівництва з самооцінки враховує вищезазначені елементи та принципи, перелічені в розділі 3.5. Насправді модель надає бали на основі значення двох параметрів, **рівня зрілості** та **коефіцієнта охоплення**. Кожен із цих параметрів можна розрахувати на різних рівнях: (i) для цілі, (ii) для кластера цілей або (iii) сукупний.

Бали на рівні цілі

Бал рівня зрілості показує рівень зрілості, демонструючи запроваджені спроможності та практику. Бал рівня зрілості розраховується як найвищий рівень, для якого респондент задовольнив усі необхідні елементи (*тобто* відповідь "ТАК" на всі необхідні запитання), крім того, він виконав усі необхідні елементи попередніх рівнів зрілості.

Коефіцієнт охоплення показує ступінь охоплення всіх показників, відповідь на які є позитивною, незалежно від їх рівня. Це додаткове значення, яке враховує всі показники, що вимірюють ціль. Коефіцієнт охоплення обчислюється як пропорція між загальною кількістю запитань у межах цілі та кількістю запитань, на які надано позитивну відповідь.

Важливо пояснити, що для решти документа слово ***"бал"*** використовується для позначення як значень рівня зрілості, так і коефіцієнта охоплення.

Рисунок 2 — механізм нарахування балів для цілі забезпечує візуалізацію механізму оцінки, описаного в розділі 3.1, який буде нижче більш детально розкритий.

Рисунок 2. Механізм нарахування балів для цілі

На рисунку 2 наведено приклад того, як розраховується рівень зрілості для цілі. Варто зазначити, що респондент виконав усі необхідні елементи перших трьох рівнів зрілості та лише частково виконав ті, що перебувають на рівні 4. Отже, бал вказує на те, що ***рівень зрілості респондента є рівнем 3 для цілі "організувати тренування з кібербезпеки"****.*

Однак у прикладі, зображеному на рисунку 2, рівень зрілості цілі не може охопити інформацію, що надається показниками, які мають позитивний бал та які перевищують рівень 3 зрілості. У цьому випадку коефіцієнт охоплення може надати огляд усіх елементів, які респондент застосував для досягнення цієї цілі, попри фактичний рівень зрілості. У цьому випадку пропорція між загальною кількістю запитань у межах цілі та кількістю запитань, на які було надано позитивну відповідь, дорівнює 19/27, тобто значення ***коефіцієнта охоплення становить 70 %.***

Крім того, з метою пристосування до особливостей країн-членів, при цьому дозволяючи також послідовний огляд, бал обчислюється за двома різними вибірками на рівні кластера та сукупному рівні:

- **загальні бали:** одна повна вибірка, що охоплює всі цілі, включені в кластер або в рамках всього керівництва (від одного до 17);
- **конкретні бали:** одна конкретна вибірка, що охоплює лише цілі, обрані країною-членом (зазвичай ті, що відповідають цілям, наявним у Національній стратегії кібербезпеки конкретної країни) у межах кластера або в рамках всього керівництва.

Бали на рівні кластера

Загальний рівень зрілості кожного кластера обчислюється як середнє арифметичне значення рівня зрілості всіх цілей у цьому кластері.

Конкретний рівень зрілості кожного кластера обчислюється як середнє арифметичне значення рівня зрілості цілей у межах такого кластера, який вирішила оцінити країна-член (зазвичай це відповідає цілям, наявним у Національній стратегії кібербезпеки конкретної країни).

Наприклад, на рисунку 1 показано, що кластер (I) управління та стандарти кібербезпеки складається з трьох цілей. Якщо припустити, що респондент вирішив оцінити лише перші дві цілі, але не третю, і припустивши, що перші дві цілі мають рівень зрілості 2 та 4 відповідно, то рівень зрілості кластера з урахуванням усіх цілей — це рівень 2 (загальний рівень зрілості кластера (I) = (2 + 4) / 3), тоді як рівень зрілості кластера з урахуванням лише конкретних цілей, обраних оцінювачем, становить рівень 3 (конкретний рівень зрілості кластера (I) = (2 + 4) / 2).

Загальний коефіцієнт охоплення кожного кластера обчислюється як пропорція між загальною кількістю запитань у межах кластера та кількістю запитань, на які надано позитивну відповідь.

Конкретний коефіцієнт охоплення кожного кластера обчислюється як пропорція між загальною кількістю запитань у межах кластера, що стосуються цілей, які країна-член вирішила оцінити (як правило, це відповідає цілям, зазначеним у Національній стратегії кібербезпеки конкретної країни), та кількістю запитань, на які надано позитивну відповідь.

Бали на сукупному рівні

Сукупний загальний рівень зрілості країни обчислюється як середнє арифметичне значення рівня зрілості всіх цілей у рамках керівництва, від одного до 17.

Сукупний конкретний рівень зрілості країни обчислюється як середнє арифметичне значення рівня зрілості цілей у межах керівництва, які вирішила оцінити країна-член (зазвичай це відповідає цілям, наявним у Національній стратегії кібербезпеки конкретної країни).

Сукупний загальний коефіцієнт охоплення країни обчислюється як пропорція між загальною кількістю запитань у межах усіх цілей, включених до керівництва (від одного до 17), та кількістю запитань, на які надано позитивну відповідь.

Сукупний конкретний коефіцієнт охоплення країни обчислюється як пропорція між загальною кількістю запитань у межах цілей керівництва, які держава-член обрала для оцінки (зазвичай це відповідає цілям, наявним у Національній стратегії кібербезпеки конкретної країни), та кількістю запитань, на які надано позитивну відповідь.

Для кожного показника респонденти можуть обрати третій варіант «не знаю/не застосовується» для своєї відповіді. У цьому випадку показник виключається із загального підрахунку результатів.

Рівні зрілості на рівні кластера та сукупному рівні обчислюються із середнім арифметичним, аби показати прогрес між двома оцінками. Насправді альтернатива, що полягає в обчисленні рівнів зрілості для кластера та сукупного рівня зрілості як рівня зрілості найменш зрілої цілі - хоча і є релевантною з погляду зрілості, не може враховувати прогрес, досягнутий у сферах, охоплених іншими цілями.

Оскільки рівень кластера та сукупний рівень консолідовані для цілей звітування, було зроблено вибір використовувати середнє арифметичне значення. Для більшої точності для цілей звітування використовуйте бали на рівні цілі.

На рисунку 3 нижче узагальнено механізми нарахування балів на різних рівнях моделі (ціль, кластер, сукупний).

Рисунок 3. Механізм нарахування сукупного бала

3.5 ВИМОГИ ДО КЕРІВНИЦТВА З САМООЦІНКИ

Представлене в цьому розділі керівництво з оцінки національних спроможностей базується на потребах, окреслених країнами-членами, і розроблене з урахуванням низки вимог, перелічених нижче.

- КОНС впроваджується країною-членом на добровільних засадах як керівництво з самооцінки.
- КОНС націлене на вимірювання спроможностей кібербезпеки країн-членів стосовно 17 цілей. Однак країна-член може вибрати цілі, які вона хоче оцінити, та оцінювати лише певну групу цілей з усіх 17 цілей.
- Керівництво з самооцінки спрямоване на вимірювання рівня зрілості спроможностей кібербезпеки країни-члена.
- Результати оцінки не публікуються, якщо країна-член не вирішить це зробити за власною ініціативою.
- Країна-член може показати результати оцінки, представляючи рівень зрілості спроможностей кібербезпеки країни, кластера цілей або навіть однієї цілі.
- Усі оцінені цілі однаково актуальні в рамках керівництва з оцінки, отже, вони мають однакову важливість. Те саме стосується показників, розміщених у ньому.
- Країна-член може відстежувати свій прогрес з часом.

Керівництво з самооцінки спрямоване на підтримку країн-членів у розбудові спроможностей кібербезпеки. Отже, воно також включає набір рекомендацій або настанов для скерування європейських країн щодо вдосконалення їх рівня зрілості.

Примітка: ці рекомендації або настанови є загальними на основі публікацій ENISA та надбаного досвіду від інших країн і будуть базуватися на результатах самооцінки.

4. ПОКАЗНИКИ КОНС

4.1 ПОКАЗНИКИ КЕРІВНИЦТВА З ОЦІНКИ

У цьому розділі представлені показники Керівництва ENISA з оцінки національних спроможностей. Наступні розділи організовані за кластерами.

Для кожного кластера в таблиці представлений вичерпний набір показників у формі запитань, що репрезентують певний рівень зрілості. Анкета є основним інструментом самооцінки. Слід вказати на два набори показників для кожної цілі:

- набір загальних запитань щодо зрілості стратегії (9 загальних запитань), позначених від «a» до «c» для кожного рівня зрілості, що повторюються для кожної цілі; і
- набір запитань щодо спроможності кібербезпеки (319 запитань щодо спроможності кібербезпеки), пронумерованих від «1» до «10» для кожного рівня зрілості, що конкретизовані для сфери, охопленої ціллю.

Кожне запитання подається з позначкою (0–1), яка вказує, чи це питання з необхідним показником (1) або з необов'язковим показником (0) для рівня зрілості.

Кожне запитання можна ідентифікувати за ідентифікаційним номером, що складається з:

- номера цілі,
- рівня зрілості та
- номера запитання.

Наприклад, ідентифікаційний номер запитання 1.2.4 означає четверте запитання рівня зрілості 2 стратегічної цілі (I) "розробити національні плани реагування на інциденти кібербезпеки".

Слід зазначити, що всі запитання анкети стосуються національного рівня, якщо не зазначено інше. У всіх запитаннях займенник "ви" в загальних рисах стосується країни-члена, а не особи чи державного органу, що проводить оцінку.

Визначення кожної цілі можна знайти в главі 2.2 «Спільні цілі, визначені в національних стратегіях ЄС щодо безпеки мережевих та інформаційних систем»

4.1.1 Кластер № 1: управління та стандарти кібербезпеки

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
1 — розробити національні плани реагування на інциденти кібербезпеки	a	Чи охоплює цю ціль ваша чинна Національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи розпочали ви працювати над розробкою національних планів реагування на інциденти кібербезпеки? *Наприклад,* викладення загальних цілей, сфери застосування та/або принципів планів реагування на інциденти тощо.	1	Чи є у вас доктрина/національна стратегія, яка включає кібербезпеку як фактор кризової ситуації (тобто проєкт, політика тощо)?	1	Чи є у вас план управління кіберкризами на національному рівні?	1	Чи задоволені ви кількістю або відсотком критично важливих секторів, включених до національного плану реагування на інциденти кібербезпеки?	1	Чи є у вас процес вивчення надбаного досвіду після тренувань з кібербезпеки чи реальних криз на національному рівні?	1
	2	Чи загальновідомо, що кіберінциденти є фактором кризової ситуації, який може загрожувати національній безпеці?	0	Чи є у вас центр для отримання інформації та інформування осіб, що приймають 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 є у вас процедури на національному рівні, спрямовані на вирішення кіберкриз?	1	Чи достатньо часто ви організовуєте заходи (тобто тренування), пов'язані з національним плануванням реагування на інциденти кібербезпеки?	1	Чи є у вас процес регулярного тестування національного плану?	1
	3	Чи проводились дослідження (технічні, оперативні, політичні) 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 є у вас команда комунікацій, спеціально підготовлена для реагування на кіберкризи та інформування громадськості?	1	Чи достатньо у вас людей, що займаються плануванню кризових ситуацій, вивченням надбаного досвіду та впровадженням змін?	1	Чи є у вас адекватні інструменти та платформи для формування ситуативної обізнаності?	1
	4	–		Чи є у вас на національному рівні методологія оцінки кіберзагрози, яка включає процедури оцінки впливу?	0	Чи залучаєте ви всіх відповідних національних зацікавлених осіб (служби національної безпеки, оборони, цивільного захисту, правоохоронні органи, міністерства, органів влади тощо?)	1	Чи достатньо у вас 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	–		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 особами в ЄС у разі потреби?	0	–		–	
	7	–		–		Чи взаємодієте ви з міжнародними зацікавленими особами з країн, які не є членами ЄС, у разі потреби?	0	–		–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
2 — встановити базові заходи безпеки	a	Чи охоплює цю ціль ваша чинна Національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи проводили ви 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 заходи безпеки відповідно до міжнародних/національних стандартів?	1	Чи є базові заходи безпеки обов'язковими?	1	Чи існує процес частого оновлення базових заходів безпеки?	1	Чи є у вас процес для посилення ІКТ, коли не вдається зреагувати й розв'язати інциденти за допомогою заходів?	1
	2	Чи проводили ви 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 при визначенні базових заходів безпеки?	1	Чи застосовуєте ви горизонтальні заходи безпеки у критично важливих секторах?	1	Чи впроваджений механізм моніторингу для вивчення застосування базових заходів безпеки?	1	Чи оцінюєте ви доречність нових стандартів, які розробляються у відповідь на останні зміни в середовищі загроз?	1
	3	–		–		Чи застосовуєте ви галузеві заходи безпеки у критично важливих секторах?	1	Чи існує національний орган, який перевіряє виконання базових заходів безпеки?	1	Чи маєте або чи сприяєте ви реалізації національному процесу координованого розкриття інформації про вразливість (CVD)?	1
	4	–				Чи відповідають базові заходи безпеки застосовним схемам сертифікації?	1	Чи запровадили ви процес виявлення протягом певного проміжку часу організацій, які не дотримуються вимог?	1	–	
	5	–		–		Чи запроваджений процес оцінки власного ризику для базових заходів безпеки?	1	Чи є процес аудиту для забезпечення належного застосування заходів безпеки?	1	–	
	6	–		–		Чи аналізуєте ви обов'язкові базові заходи безпеки в процесі закупівель державними органами?	0	Чи встановлюєте ви або активно заохочуєте ухвалення стандартів безпеки для розробки критично важливих ІТ/ООП продуктів (медичне обладнання, підключені до мережі та автономні транспортні засоби, професійне радіо, обладнання важкої промисловості тощо)?	0	–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
3 — забезпечити захист цифрової ідентифікації та зміцнення довіри до цифрових державних послуг	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи проводили ви дослідження або аналіз прогалин з метою визначення потреб у забезпеченні захисту цифрових державних послуг для громадян і бізнесу?	1	Чи проводите ви 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 сприяєте ви впровадженню методологій з вбудованим алгоритмом конфіденційності у всіх проєктах електронного урядування?	1	Чи збираєте ви показники щодо інцидентів у сфері кібербезпеки, пов'язаних із порушенням цифрових державних послуг?	1	Чи берете ви участь в європейських 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 маєте ви стратегію побудови або сприяння впровадженню безпечних національних схем електронної ідентифікації (eID) для громадян і бізнесу?	1	Чи залучаєте ви приватних зацікавлених осіб до процесу розробки та надання безпечних цифрових державних послуг?	1	Чи впроваджували ви взаємне визнання засобів електронної ідентифікації з іншими країнами-членами?	1	Чи берете ви активну участь в експертних оглядах, що є частиною повідомлень Європейській комісії про схеми електронної ідентифікації?	1
	3	–		Чи маєте ви стратегію 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 впроваджуєте ви мінімальний базовий рівень безпеки для всіх цифрових державних послуг?	1	–		–	
	4	–		Чи є у вас стратегія щодо хмар електронного урядування (стратегія хмарних технологій, спрямована на уряд та державні органи, такі як 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 у Додатку до Регламенту eIDAS (ЄС) № 910/2014?	1	–		–	
	5	–		–		Чи є у вас цифрові державні послуги, що вимагають схем електронної ідентифікації зі значним або високим рівнем безпеки, як визначено у Додатку до Регламенту eIDAS (ЄС) № 910/2014?	1	–		–	
	6	–		–		Чи є у вас постачальники довірчих послуг для громадян і бізнесу (електронні підписи, електронні печатки, реєстрована електронна доставка, присвоєння мітки часу, автентифікація вебсайту)?	1	–		–	
	7	–		–		Чи сприяєте ви прийняттю базових заходів безпеки для всіх моделей розгортання хмар обчислення (наприклад, Private, Public, Hybrid, IaaS, PaaS, SaaS)?	0	–		–	

4.1.2 Кластер № 2: розбудова спроможностей та обізнаність

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
4 — встановити спроможність реагування на інциденти	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи є у вас неформальні спроможності реагування на інциденти, якими управляє державний або приватний сектори або спільне керування між ними?	1	Чи є у вас хоча б одна офіційна національна команда CSIRT?	1	Чи є у вас спроможності реагування на інциденти для секторів, зазначених у Додатку II до Директиви NIS?	1	Чи визначили ви та чи сприяли запровадженню стандартизованої практики для процедур реагування на інциденти та схем класифікації інцидентів?	1	Чи є у вас механізми раннього виявлення, ідентифікації, запобігання, реагування та пом'якшення наслідків щодо вразливостей нульового дня?	1
	2	–		Чи мають ваші національні команди CSIRT чітко визначений обсяг втручання? Наприклад, залежно від цільового сектору, типів інцидентів, наслідків.	1	Чи існує у вашій країні механізм співпраці команди CSIRT для реагування на інциденти?	1	Чи оцінюєте ви свою 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 ваші 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 ваші 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	–		–	
	5	–		–		Чи формально ви визначили чітку політику та процедури щодо обробки інцидентів?	1	–		–	
	6	–		–		Чи беруть участь ваші національні команди CSIRT у тренуваннях з кібербезпеки як на національному, так і на міжнародному рівні?	1	–		–	
	7	–		–		Чи долучена ваша національна команда CSIRT до FIRST (Форум команд реагування на інциденти та забезпечення безпеки)?	0	–		–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
5 — підвищити обізнаність користувачів	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи є мінімальне визнання з боку уряду, приватного сектору або загальних користувачів, що існує потреба підвищити обізнаність щодо питань кібербезпеки та конфіденційності?	1	Чи визначили ви конкретну цільову аудиторію для підвищення обізнаності користувачів? Наприклад, загальні користувачі, молодь, бізнес-користувачі (які можна додатково розподілити на МСП, ООП, ПЗО тощо).	1	Чи розробили ви комунікаційні плани/стратегію для кампаній?	1	Чи складаєте ви метрики для оцінки вашої кампанії на етапі планування?	1	Чи запроваджені у вас механізми для забезпечення постійної актуальності кампаній з 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 складаєте ви план заходів щодо підвищення обізнаності з питань інформаційної безпеки та конфіденційності?	1	Чи є у вас процес створення контенту на державному рівні?	1	Чи оцінюєте ви свої кампанії після їх виконання?	1	Чи проводите ви періодичну оцінку чи дослідження для вимірювання зміни ставлення чи зміни поведінки стосовно питань кібербезпеки та конфіденційності у приватному та державному секторах?	1
	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 у вас ресурси, доступні та легко впізнанні (наприклад, єдиний Інтернет-портал, набір інструментів з підвищення обізнаності) для користувачів, які прагнуть освоїти інформацію щодо питань кібербезпеки та конфіденційності?	1	Чи є у вас механізми для визначення цільових галузей для підвищення обізнаності (тобто середовище загроз ENISA, національні середовища, міжнародні середовища, відгуки національних центрів боротьби з кіберзлочинністю тощо)?	1	Чи запроваджені у вас 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 консультуєтесь ви з поведінковими експертами, аби адаптувати вашу кампанію до цільової аудиторії?	1
	4	–		–		Чи збираєте ви разом зацікавлених осіб з експертами та командами комунікацій для створення контенту?	1			–	
	5	–		–		Чи залучаєте ви та співпрацюєте з приватним сектором щодо вашої дільності в рамках інформаційних кампаній і поширення повідомлень серед ширшої аудиторії?	1	–		–	
	6	–		–		Чи готуєте ви конкретні ініціативи щодо підвищення обізнаності для керівників державного, приватного, академічного або громадянського секторів?	1	–		–	
	7	–		–		Чи берете ви участь у кампаніях європейського місяця кібербезпеки (ECSM) ENISA?	0	–		–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
6 — організувати тренування з кібербезпеки	a	Чи охоплює цю ціль ваша чинна Національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи проводите ви кризові тренування в інших секторах (крім кібербезпеки) на національному або загальноєвропейському рівні?	1	Чи є у вас програма тренування з кібербезпеки на національному рівні?	1	Чи залучаєте ви всі відповідні органи державного управління? (навіть якщо сценарій притаманний певному сектору)	1	Чи пишете ви звіти після закінчення дій/звіти про оцінку?	1	Чи є у вас спроможність проводити аналіз надбаного досвіду у кіберсфері (процеси звітування, аналіз, пом'якшення наслідків)?	1
	2	Чи є у вас ресурси, виділені для розробки та планування навчання з управління кризовими ситуаціями?	1	Чи проводите ви або чи надаєте пріоритет тренуванням з управління кіберкризами щодо життєво важливих соціальних функцій та критично важливої інфраструктури?	1	Чи залучаєте ви приватний сектор до планування та виконання тренувань?	1	Чи перевіряєте ви плани та процедури національного рівня?	1	Чи є у вас налагоджений процес реєстрації надбаного досвіду?	1
	3	–		Чи визначили ви координаційний орган для нагляду за розробкою та плануванням тренувань з кібербезпеки (державне агентство, консультування тощо)?	0	Чи організовуєте ви секторальні тренування на національному та/або міжнародному рівні?	1	Чи берете ви участь у тренуваннях з кібербезпеки на загальноєвропейському рівні?	1	Чи адаптуєте ви сценарії навчань залежно від останніх надбань (технологічні досягнення, глобальні конфлікти, середовище загроз тощо)?	1
	4	–		–		Чи організовуєте ви тренування у всіх критичних секторах, згаданих у Додатку II до Директиви NIS?	1	–		Чи узгоджуєте ви свої процедури управління кризовими ситуаціями з іншими країнами-членами для забезпечення ефективного загальноєвропейського управління кризовими ситуаціями?	1
	5	–		–		Чи організовуєте ви міжгалузеві тренування з кібербезпеки?	1	–		Чи впроваджений у вас механізм швидкої адаптації стратегії, планів та процедур з огляду на надбаний досвід після тренувань?	0
	6	–		–		Чи організовуєте ви тренування з кібербезпеки, характерні для різних рівнів? (технічний та оперативний рівень, рівень процедури, рівень прийняття рішень, політичний рівень тощо)	0	–		–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
7 — посилити навчальні та освітні програми	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи розглядаєте Ви розробку навчальних та освітніх програм з кібербезпеки?	1	Чи запроваджуєте ви курси, присвячені кібербезпеці?	1	Чи охоплена у вашій країні культура кібербезпеки на ранній стадії навчального процесу? Наприклад, чи запроваджені у вас курси з кібербезпеки в середній школі та старшій школі?	1	Чи спонукаєте ви персонал у приватному та державному секторі стати акредитованими або сертифікованими фахівцями?	1	Чи запроваджені у вас механізми, що забезпечують постійну актуальність тренінгів та освітніх програм щодо сучасних та нових технологічних розробок, змін у середовищі загроз, правових норм і директив з національної безпеки?	1
	2	–		Чи пропонують університети вашої країни підготовку кандидатів наук у галузі кібербезпеки як самостійну дисципліну, а не як галузь інформатики?	1	Чи є у вас національні дослідницькі лабораторії та освітні установи, які спеціалізуються на кібербезпеці?	1	Чи розроблені у вашій країні програми навчання або наставництва з питань кібербезпеки для підтримки національних стартапів та МСП?	1	Чи створюєте ви академічні центри підвищення кваліфікації в галузі кібербезпеки, які виступають центрами досліджень та освіти?	1
	3	–		Чи плануєте ви навчати освітян, незалежно від їх галузі, з питань інформаційної безпеки та конфіденційності? *Наприклад,* безпека в Інтернеті, захист персональних даних, кіберзнущання.	1	Чи заохочуєте/фінансуєте ви спеціальні курси з питань кібербезпеки та навчальні плани для працівників агентств з працевлаштування країн-членів?	1	Чи активно ви сприяєте додаванню курсів з інформаційної безпеки у 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 є у вас курси та/або спеціалізована програма з кібербезпеки для 5–8 рівнів EQF (Європейська рамка кваліфікацій)?	1	Чи регулярно ви оцінюєте недоліки професійної підготовки (нестачу працівників сфери кібербезпеки) в галузі інформаційної безпеки?	1	–	
	5	–		–		Чи заохочуєте ви та/або підтримуєте ініціативи щодо включення курсів безпеки в Інтернеті в освіту на початковому та середньому рівнях?	1	Чи сприяєте ви розвитку мереж та обміну інформацією між науковими установами як на національному, так і на міжнародному рівні?	1		
	6	–		–		Чи фінансуєте ви або пропонуєте безплатні базові тренінги з кібербезпеки для громадян?	0	Чи залучаєте ви приватний сектор у будь-якій формі до освітніх ініціатив з питань кібербезпеки? Наприклад, до розробки та проведення курсів, стажування, працевлаштування тощо.	1	–	
	7	–		–		Чи організовуєте ви щорічні заходи з інформаційної безпеки (наприклад, змагання хакерів чи хакатони)?	0	Чи впроваджуєте ви механізми фінансування для заохочення отримання ступенів з кібербезпеки? *Наприклад,* стипендії, гарантоване стажування / практика, гарантована робота в конкретній галузі або на посадах в державному секторі.	0	–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
8 — сприяти науково-дослідним і дослідно-конструкторським роботам	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи проводили ви дослідження або аналізи для визначення пріоритетів НДДКР у галузі кібербезпеки?	1	Чи є у вас процес визначення пріоритетів НДДКР (наприклад, нові можливості для стримування, захисту, виявлення та адаптації до нових видів кібератак)?	1	Чи є у вас план як пов'язати проєкти НДДКР з реальною економікою?	1	Чи відповідають проєкти НДДКР з кібербезпеки відповідним стратегічним цілям, наприклад, DSM, H2020, Цифрова Європа, Стратегія кібербезпеки ЄС?	1	Чи продовжуєте ви співпрацювати на національному рівні з будь-якими міжнародними проєктами НДДКР, пов'язаними з кібербезпекою?	1
	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 у вас місцеві/регіональні екосистеми стартапів та інші канали взаємодії (наприклад, технологічні парки, інноваційні кластери, події/платформи з нетворкінгу) для сприяння інноваціям (у тому числі для стартапів з кібербезпеки)?	1	Чи існують угоди про співпрацю з університетами та іншими науково-дослідними установами?	1	Чи берете ви участь у 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 є у вас кафедри промислових досліджень в університетах, аби поєднувати теми досліджень і потреби ринку?	1	–		–	
	6	–		–		Чи є у вас спеціальні програми фінансування НДДКР у сфері кібербезпеки?	0	–		–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
9 — забезпечити стимули для приватного сектору інвестувати в заходи безпеки	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи наявна промислова політика або політична воля для заохочення розвитку галузі кібербезпеки?	1	Чи бере участь приватний сектор у розробці стимулів?	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 фокусуєте ви стимули на можливостях кібербезпеки залежно від останніх подій, пов'язаних із загрозами?	1
	2	–		Чи визначили ви конкретні можливості кібербезпеки, які слід розробляти? *Наприклад,* криптографія, приватність, нова форма автентифікації, ШІ для кібербезпеки тощо.	0	Чи надаєте ви підтримку (наприклад, податкові пільги) для стартапів і МСП, що займаються кібербезпекою?	1	Чи стимулюєте ви приватний сектор зосередитись на безпеці передових технологій? *Наприклад,* 5G, штучний інтелект, інтернет речей, квантові обчислення тощо.	1	–	
	3	–		–		Чи надаєте ви податкові пільги або іншу фінансову мотивацію інвесторам приватного сектору в стартапах з кібербезпеки?	1	–		–	
	4	–		–		Чи сприяєте ви доступу стартапам і МСП, що займаються кібербезпекою, до процесу державних закупівель?	0	–		–	
	5	–		–		Чи є бюджет для стимулювання приватного сектору?	0	–		–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
10 — покращити кібербезпеку ланцюга постачання	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи проводили ви дослідження кращих практик безпеки в галузі управління ланцюгами постачання, що використовуються для закупівель у різних сегментах промисловості та/або в державному секторі?	1	Чи проводите ви 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 використовуєте ви схему сертифікації безпеки для продуктів і сервісів, заснованих на ІКТ? *Наприклад,* Група SOG-IS MRA в Європі (Група старших офіцерів з питань безпеки інформаційних систем в рамках Угоди про взаємне визнання), Угода про визнання спільних критеріїв (CCRA), національні проєкти, галузеві проєкти тощо.	1	Чи запроваджений у вас процес оновлення оцінок кібербезпеки в ланцюгу постачання сервісів і продуктів ІКТ у критично важливих секторах (як зазначено в Додатку II Директиви NIS (2016/1148))?	1	Чи є у вас детекторні зонди в ключових елементах ланцюга постачання для виявлення ранніх ознак порушення нормального функціонування? *Наприклад,* контроль безпеки на рівні Інтернет-провайдера, зонди безпеки в основних компонентах інфраструктури тощо.	1
	2	–		Чи застосовуєте ви стандарти у 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 ви активно сприяєте безпеці та конфіденційності, створюючи передові практики розробки продуктів і сервісів ІКТ? *Наприклад,* безпечний життєвий цикл розробки програмного забезпечення, життєвий цикл інтернету речей.	1	Чи запроваджений у вас процес виявлення слабких ланок кібербезпеки в ланцюгу постачання критично важливих секторів (як визначено в Додатку II до Директиви NIS (2016/1148))?	1	–	
	3	–		–		Чи розробляєте та надаєте ви централізовані каталоги з розширеною інформацією про наявні стандарти інформаційної безпеки та конфіденційності, які є масштабованими для МСП та застосовуються ними?	1	Чи запроваджені у вас механізми, які гарантують, що критично важливі для ООП продукти та сервіси ІКТ є кіберстійкими (*тобто* здатність підтримувати доступність та безпеку від кіберінцидентів)? *Наприклад,* шляхом тестування, регулярних оцінок, виявлення ушкоджених елементів тощо.	1	–	
	4	–				Чи берете ви активну участь у розробці Керівництва ЄС з сертифікації цифрових продуктів, сервісів і процесів ІКТ, як це встановлено в Акті ЄС про кібербезпеку (Регламент (ЄС) 2019/881)? *Наприклад,* участь в Європейській групі з сертифікації кібербезпеки (ECCG), що просуває технічні стандарти та процедури щодо безпеки продуктів/сервісів ІКТ.	0	Чи сприяєте ви розробці схем сертифікації, орієнтованих на МСП, для підвищення інформаційної безпеки та прийняття стандартів конфіденційності?	0	–	
	5	–		–		Чи надаєте ви МСП будь-які види стимулів з метою ухвалення ними стандартів безпеки та конфіденційності?	0	Чи розроблені у вас 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 заохочуєте ви постачальників програмного забезпечення підтримувати МСП, забезпечуючи безпечні конфігурації за налаштуванням у продуктах, орієнтованих на невеликі організації?	0	–		–	

4.1.3 Кластер № 3: нормативно-правова база

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
11 — захист критично важливої інформаційної інфраструктури, ООП і ПЗО	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи є загальне розуміння того, що оператори КВІІ сприяють національній безпеці?	1	Чи є у вас методологія визначення основних послуг?	1	Чи впровадили ви Директиву NIS (2016/1148)?	1	Чи є у вас процедура оновлення реєстру ризиків?	1	Чи створюєте та оновлюєте ви звіти про середовище загроз?	1
	2	–		Чи є у вас методологія ідентифікації КВІІ?	1	Чи впроваджували ви Директиву ECI (2008/114) про ідентифікацію та позначення європейських критичних інфраструктур та оцінку необхідності вдосконалення їх захисту?	1	Чи запроваджені у вас інші механізми, що дозволяють виміряти, чи технічні й організаційні заходи, впроваджені ООП, 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, такі як детекторні зонди або аналіз конфігурації для конкретної системи тощо.	1	Залежно від останніх подій у середовищі загроз чи можете ви включити новий сектор у свій план дій щодо захисту КВІІ?	1
	3	–		Чи є у вас методологія визначення ООП?	1	Чи маєте ви національний реєстр визначених ООП для критичного сектору?	1	Чи аналізуєте та, відповідно, оновлюєте ви перелік визначених ООП щонайменше раз на два роки?	1	Залежно від останніх подій у середовищі загроз чи можете ви внести нові вимоги у свій план дій щодо захисту КВІІ?	1
	4	–		Чи є у вас методологія визначення постачальників цифрових послуг?	1	Чи маєте ви національний реєстр визначених постачальників цифрових послуг?	1	Чи запроваджені у вас інші механізми, що дозволяють виміряти, чи технічні й організаційні заходи, впроваджені постачальниками цифрових послуг, 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, такі як детекторні зонди або аналіз конфігурації для конкретної системи тощо.	1		
	5	–		Чи є у вас 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 є у вас національний реєстр ризиків для виявлених або відомих ризиків?	1	Чи аналізуєте та, відповідно, оновлюєте ви перелік визначених постачальників цифрових послуг щонайменше раз на два роки?	1	–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
11 — захист критично важливої інфраструктури, ООП і ПЗО	6	–		Чи розробляєте ви секторальні плани захисту? Наприклад, базові заходи з кібербезпеки (обов'язкові або настанови).	0	Чи є у вас методологія картографування взаємозалежностей КВІІ?	1	Чи використовуєте ви схему сертифікації безпеки (національну або міжнародну), аби допомогти ООП та постачальникам цифрових послуг ідентифікувати безпечні продукти ІКТ? Наприклад, Група SOG-IS MRA в Європі, національні проєкти тощо.	1	–	
	7	–		–		Чи застосовуєте ви практику управління ризиками для виявлення, кількісного визначення та управління ризиками, пов'язаними з КВІІ, на національному рівні?	1	Чи використовуєте ви схему сертифікації безпеки або процедуру кваліфікації для оцінки постачальників послуг, які працюють з ООП? Наприклад, постачальники послуг у сфері виявлення інцидентів, реагування на інциденти, аудит кібербезпеки, хмарні сервіси, комп'ютеризовані карти тощо.	1	–	
	8	–		–		Чи берете ви участь у консультаційному процесі для виявлення транскордонних взаємозалежностей?	1	Чи запроваджені у вас механізми для вимірювання рівня відповідності ООП та постачальників цифрових послуг з огляду дотримання базових заходів кібербезпеки?	0	–	
	9					Чи є у вас єдиний координатор, відповідальний за координацію питань, що стосуються безпеки мережевих та інформаційних систем на національному рівні та в рамках транскордонного співробітництва на рівні Союзу?	1	Чи ухвалені у вас розпорядження щодо забезпечення безперервності сервісів, які надаються критично важливими інформаційними інфраструктурами? Наприклад, передбачення кризи, процедури відновлення критично важливих інформаційних систем, безперервність бізнесу без ІТ, процедури резервного копіювання і переміщення даних у режим офлайн тощо.	0		
	10					Чи визначаєте ви 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 надаєте ви інструменти або методології для виявлення кіберінцидентів?	1	–		–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
12 — займатися протидією кіберзлочинності	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи проводили ви дослідження з метою виявлення вимог правоохоронних органів (правової бази, ресурсів, навичок тощо) для ефективного подолання кіберзлочинності?	1	Чи повністю відповідає ваша національна законодавча база відповідній законодавчій базі ЄС, включно з Директивою 2013/40/ЄС про атаки на 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	Чи є у вас підрозділи, відповідальні за протидію кіберзлочинності в органах прокуратури?	1	Чи збираєте ви статистику згідно з положеннями статті 14 (1) Директиви 2013/40/ЄС (Директива про атаки на інформаційні системи)?	1	Чи є у вас міжвідомче навчання або тренінги для представників правоохоронних органів, суддів, прокурорів і національних/державних команд CSIRT на національному рівні та/або на багатосторонньому рівні?	1
	2	Чи проводили ви дослідження з метою виявлення вимог до прокурорів і суддів (правової бази, ресурсів, навичок тощо) для ефективного подолання кіберзлочинності?	1	Чи є у вас будь-яке законодавче положення, що стосується крадіжки особистих даних в Інтернеті та крадіжки персональних даних?	1	Чи є у вас спеціальний бюджет, виділений підрозділам з питань протидії кіберзлочинності?	1	Чи збираєте ви окрему статистику щодо кіберзлочинності? Наприклад, оперативна статистика, статистика тенденцій кіберзлочинності, статистика доходів від кіберзлочинності та завданих збитків тощо.	1	Чи берете ви 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 ваша країна Будапештську конвенцію Ради Європи про кіберзлочинність?	1	Чи є у вас які-небудь юридичні положення, що стосуються порушення інтелектуальної власності та авторського права в Інтернеті?	1	Чи створили ви центральний орган/організацію для координації діяльності у сфері боротьби з кіберзлочинністю?	1	Чи оцінюєте ви 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
	4			Чи є у вас які-небудь законодавче положення, що стосується переслідувань в Інтернеті чи кіберзнущань?	1	Чи встановили ви механізми співпраці між відповідними національними установами, які залучені до боротьби з кіберзлочинністю, в тому числі між правоохоронними органами, національними командами CSIRT?	1	Чи регулярно ви проводите оцінки, аби переконатися, що у вас є достатньо ресурсів (людських, бюджетних та інструментальних), виділених для підрозділів з питань кіберзлочинності в межах правоохоронної системи?	1	Чи сприяє ваша нормативна база співпраці між командами CSIRT / правоохоронними органами та органами правосуддя (прокурорами та суддями)?	1
	5			Чи є у вас будь-яке законодавче положення щодо боротьби з комп'ютерним шахрайством? Наприклад, дотримання положень Будапештської конвенції Ради Європи про кіберзлочинність.	1	Чи співпрацюєте та обмінюєтесь ви інформацією з іншими країнами-членами у сфері боротьби з кіберзлочинністю?	1	Чи регулярно ви проводите оцінки, аби переконатися, що у вас є достатньо ресурсів (людських, бюджетних та інструментальних), виділених для підрозділів з питань кіберзлочинності в межах органів прокуратури?	1	Чи берете ви участь у створенні та підтримці стандартизованих інструментів і методологій, форм і процедур, якими можна ділитися із зацікавленими особами з ЄС (правоохоронними органами, командами CSIRT, ENISA, ЄСЗ Європолу тощо)?	1
	6	–		Чи є у вас 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 співпрацюєте ви та обмінюєтесь інформацією з агентствами ЄС (наприклад, Європолом ЄСЗ, Євроюстом, ENISA) у сфері боротьби з кіберзлочинністю?	1	Чи є у вас підрозділи, спеціалізовані суди або судді, які розглядають справи про кіберзлочини?	1	Чи є у вас якісь прогресивні механізми, що утримують людей від залучення до кіберзлочинів чи участі у них?	0

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
12 — займатися протидією кіберзлочинності	7	–		Чи визначили ви оперативного національного координатора для обміну інформацією та реагування на термінові інформаційні запити інших країн-членів щодо правопорушень, визначених Директивою 2013/40/ЄС (Директива про атаки на інформаційні системи)?	1	Чи є у вас адекватні 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 є у вас якісь розпорядження щодо надання підтримки та допомоги жертвам кіберзлочинів (загальні користувачі, МСП, великі компанії)?	1	Чи використовує ваша країна 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 вашого правоохоронного органу спеціальний підрозділ з питань кіберзлочинності?	1	Чи є у вас стандартні операційні процедури для обробки електронних доказів?	1	Чи встановили ви міжвідомчу базу та механізми співпраці між усіма відповідними зацікавленими особами (наприклад, правоохоронними органами, національною командою CSIRT, органами правосуддя, спільнотою), в тому числі приватним сектором (наприклад, операторами основних послуг, постачальниками сервісів), де це доречно, для реагування на кібератаки?	1	–	
	9			Чи призначили ви відповідно до ст. 35 Будапештської конвенції цілодобового координатора?	1	Чи бере ваша країна участь у можливостях підвищення кваліфікації, які пропонують та/або підтримують агентства ЄС (наприклад, Європол, Євроюст, Європейське бюро з боротьби з шахрайством, Європейський поліційний коледж Cepol, ENISA)?	0	Чи сприяє ваша нормативна база співпраці між командами CSIRT та правоохоронними органами?	1	–	
	10	–		Чи призначили ви 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 ваша країна ухвалити 2-й додатковий протокол до Будапештської конвенції Ради Європи про кіберзлочинність?	0	Чи запроваджені у вас механізми (наприклад, інструменти, процедури) для полегшення обміну інформацією та співпраці між командами CSIRT / правоохоронними органами та, можливо, органами правосуддя (прокурорами та суддями) у сфері боротьби з кіберзлочинністю?	1	–	
	11			Чи регулярно ви проводите спеціалізоване навчання для зацікавлених осіб, які беруть участь у протидії кіберзлочинності (для правоохоронних органів, органів правосуддя, команди CSIRT)? Наприклад, серед 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.	1						
	12			Чи ратифікувала/приєдналася ваша країна до Будапештської конвенції Ради Європи про кіберзлочинність?	1			–		–	
	13	–		Чи підписала та ратифікувала Ваша країна Додатковий протокол (криміналізація актів расистського та ксенофобського характеру, вчинених за допомогою комп'ютерних систем) до Будапештської конвенції Ради Європи про кіберзлочинність?	0	–		–		–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
13 — встановити механізми звітування про інциденти	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи є у вас неформальні механізми обміну інформацією щодо інцидентів у сфері кібербезпеки між приватними організаціями та національними органами влади?	1	Чи є у вас схема звітування про інциденти для всіх секторів згідно з Додатком II до Директиви NIS?	1	Чи є у вас схема обов'язкового звітування про інциденти, яка функціонує на практиці?	1	Чи є у вас гармонізована процедура для галузевих схем звітування про інциденти?	1	Чи створюєте ви щорічний звіт про інциденти?	1
	2	–		Чи впроваджували ви вимоги щодо повідомлення для постачальників телекомунікаційних послуг відповідно до статті 40 Директиви (ЄС 2018/1972)? Директива вимагає, аби країни-члени 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 є у вас схема звітування про інциденти для інших секторів, крім тих, що передбачені Директивою NIS?	1	Чи запроваджені будь-які звіти про середовище кібербезпеки чи інші види аналізу, підготовлені організацією, яка отримує звіти про інциденти?	1
	3	–		Чи впроваджували ви 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 постачальники довірчих послуг повідомляли наглядовий орган про значні інциденти/порушення.	1	Чи є у вас адекватні інструменти для забезпечення конфіденційності та цілісності інформації, що передається через різні канали звітування?	1	Чи вимірюєте ви ефективність процедур звітування про інциденти? *Наприклад*, показники інцидентів, щодо яких було звітування за допомогою відповідних каналів, час подання звіту про інцидент тощо.	1	–	
	4	–		Чи впроваджували ви 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, яку вони пропонують в межах Союзу.	1	Чи є у вас платформа/інструмент для полегшення процесу звітності?	0	Чи є у вас загальна систематизація на національному рівні для класифікації інцидентів та категорій першопричин?	0	–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
14 — посилити захист конфіденційності даних	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи проводили ви дослідження або аналізи для виявлення сфер вдосконалення для кращого захисту прав приватності громадян?	1	Чи бере участь національний орган з питань захисту даних, пов'язаних з питаннями кібербезпеки (наприклад, розробка проєктів нових законів і положень про кібербезпеку, визначення мінімальних заходів безпеки)?	1	Чи пропагуєте ви передові практики щодо заходів безпеки та захисту даних спеціально для державного та/або приватного сектору?	1	Чи ви регулярно проводите оцінки, аби переконатися, що у вас є достатньо ресурсів (людських, бюджетних та інструментальних), призначених для органу з питань захисту даних?	1	Чи запроваджені у вас механізми для моніторингу останніх технологічних розробок з метою адаптації відповідних настанов і законодавчих положень/зобов'язань?	1
	2	Чи розробили ви правову базу на національному рівні 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 запускаєте ви програми з підвищення обізнаності та навчання стосовно цієї теми?	1	Чи заохочуєте ви організації та підприємства проходити сертифікацію на відповідність ISO/IEC 27701:2019 щодо Системи управління інформаційною безпекою конфіденційних даних (СУІБ)?	1	Чи берете ви активну участь/сприяєте НДДКР проєктам щодо технологій підвищення конфіденційності (PET)?	0
	3	–		–		Чи координуєте ви процедури звітування про інциденти з положеннями Закону про захист інформації (DPA)?	1	–		–	
	4	–		–		Чи сприяєте та підтримуєте ви розробку технічних стандартів з інформаційної безпеки та конфіденційності? Чи вони спеціально розроблені для малих та середніх підприємств (МСП)?	0	–		–	
	5	–		–		Чи надаєте ви практичні та масштабовані настанови щодо підтримки різних типів контролерів даних стосовно виконання законодавчих вимог та зобов'язань щодо конфіденційності та захисту даних?	0	–		–	

4.1.4 Кластер № 4: співпраця

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
15 — встановити державно-приватне партнерство (ДПП)	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи це загальновідомо, що ДПП сприяє підвищенню рівня кібербезпеки в країні за допомогою різних засобів? *Наприклад,* обмін інтересами у зростанні галузі кібербезпеки, співпраця у створенні відповідної нормативної бази з питань кібербезпеки, сприяння НДДКР тощо.	1	Чи маєте ви національний план дій щодо встановлення ДПП?	1	Чи встановили ви державно-приватне партнерство на національному рівні?	1	Чи створили ви міжгалузеве ДПП?	1	Залежно від останніх технологічних та регуляторних розробок чи можете ви адаптувати або створити ДПП?	1
	2	–		Чи визначаєте ви юридичну або договірну основу (конкретні закони, договори про нерозголошення, інтелектуальну власність) для охоплення сфери ДПП?	1	Чи створили ви ДПП, притаманне певній галузі?	1	Чи ви також зосереджуєтеся на державно-державній та приватно-приватній співпраці у створеному ДПП?	1		
	3	–		–		Чи забезпечуєте ви фінансування для створення ДПП?	1	Чи сприяєте ви створенню ДПП серед малих і середніх підприємств (МСП)?	1	–	
	4	–		–		Чи загалом державні установи очолюють процес створення ДПП? *Тобто чи* є єдиний координатор з державного сектору, який керує та координує ДПП, чи державні органи заздалегідь домовляються про те, чого вони хочуть досягти, чи є чіткі настанови від державних адміністративних органів щодо їх потреб та обмеження для приватного сектору тощо.	1	Чи вимірюєте ви результати ДПП?	1	–	
	5	–		–		Чи є ви членом Європейської організації з кібербезпеки (ECSO) договірного державно-приватного партнерства (дДПП)?	0	–		–	
	6	–		–		Чи є у вас одне або кілька ДПП, що працюють у рамках діяльності команди CSIRT?	0	–		–	
	7					Чи є у вас одне або кілька ДПП, що працюють над питаннями захисту критично важливої інформаційної інфраструктури?	0				
	8	–		–		Чи є у вас одне або кілька ДПП, що працюють над підвищенням рівня обізнаності та розвитку навичок у сфері кібербезпеки?	0	–		–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
16 — надати інституційний характер співпраці між державними органами	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи є у вас неформальні канали співпраці між державними установами?	1	Чи є у вас національна схема співпраці, орієнтована на кібербезпеку? *Наприклад,* консультативні ради, координаційні групи, форуми, ради, кіберцентри або групи експертів.	1	Чи беруть участь органи державної влади у схемі співпраці?	1	Чи забезпечуєте ви наявність каналів співпраці у сфері кібербезпеки принаймні між такими державними органами: спецслужбами, внутрішніми правоохоронними органами, органами прокуратури, урядовими суб'єктами, національною командою CSIRT та військовими?	1	Чи надається державним установам узагальнена мінімальна інформація про останні події в середовищі загроз та ситуативна обізнаність щодо кібербезпеки?	1
	2	–		–		Чи створили ви платформи співпраці для обміну інформацією?	1	Чи вимірюєте ви успіхи та обмеження різних схем співпраці щодо сприяння ефективній співпраці?	1	–	
	3	–		–		Чи визначили ви сферу дії платформи для співпраці (наприклад, завдання та обов'язки, кількість проблемних галузей)?	1	–		–	
	4	–		–		Чи організовуєте ви щорічні зустрічі?	1	–		–	
	5	–		–		Чи є у вас механізми співпраці між компетентними органами в географічних регіонах? *Наприклад,* мережа кореспондентів з питань безпеки по регіонах, офіцери з питань кібербезпеки в регіональних економічних палатах тощо.	1	–		–	

Ціль національної стратегії кібербезпеки	№	Рівень 1	R	Рівень 2	R	Рівень 3	R	Рівень 4	R	Рівень 5	
17 — долучатися до міжнародної співпраці (не тільки з країнами — членами ЄС)	a	Чи охоплює цю ціль ваша поточна національна стратегія кібербезпеки або чи плануєте ви включити її до наступної версії стратегії?	1	Чи існують неформальна практика або заходи, до яких вдаються для досягнення цілі в неузгоджений спосіб?	1	Чи є у вас план дій, який офіційно визначений та задокументований?	1	Чи переглядаєте ви свій план дій щодо цілі, аби перевірити ефективність її реалізації?	1	Чи є у вас впроваджені механізми, що забезпечують динамічну адаптацію плану дій до екологічно сталого розвитку?	1
	b			Чи визначили ви заплановані результати, керівні принципи або ключові напрями діяльності у вашому плані дій?	1	Чи маєте ви план дій з чітким розподілом ресурсів та управлінням?	1	Чи переглядаєте ви свій план дій щодо цілі, аби переконатися, що вона правильно оптимізована і щодо неї правильно визначено пріоритет?	1		
	c			Якщо це доречно, то чи реалізований ваш план дій і чи він уже дієвий у рамках обмеженого обсягу?	0						
	1	Чи маєте ви стратегію міжнародної взаємодії?	1	Чи маєте ви угоди про співпрацю з іншими країнами (двосторонні, багатосторонні) чи партнерами в інших країнах? *Наприклад,* щодо обміну інформацією, розбудови спроможностей, допомоги тощо.	1	Чи обмінюєтесь ви інформацією на стратегічному рівні? *Наприклад,* політика високого рівня, сприйняття ризику тощо.	1	Чи залучені національні державні установи з питань кібербезпеки у вашій країні до програм міжнародного співробітництва?	1	Чи ведете ви обговорення однієї або багатьох тем у рамках багатосторонніх угод?	1
	2	Чи є у вас неформальні канали співпраці з іншими країнами?	1	Чи є у вас 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 обмінюєтесь ви інформацією на тактичному рівні? *Наприклад,* відомості про зловмисників, Центри обміну та аналізу інформації, тактика, методи та процедури тощо.	1	Чи регулярно ви оцінюєте результати проєктів міжнародного співробітництва?	1	Чи ведете ви обговорення однієї чи багатьох тем у рамках міжнародних договорів чи конвенцій?	1
	3	Чи висловило державне керівництво намір брати участь у міжнародному співробітництві у сфері кібербезпеки?	1	Чи є у вас спеціальні фахівці, які беруть участь у міжнародному співробітництві?	1	Чи обмінюєтесь ви інформацією на оперативному рівні? *Наприклад,* інформацією про оперативну координацію, поточні інциденти, контролери IOC тощо.	1	–		Чи ведете ви 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 з питань інформаційної безпеки (GGE) тощо.	1
	4	–		–		Чи берете ви участь у міжнародних навчаннях з кібербезпеки?	1	–		–	
	5	–		–		Чи берете ви участь у міжнародних проєктах щодо розбудови спроможностей? *Наприклад,* тренінги, програми з розвитку навичок, створення проєктів стандартних процедур тощо.	0	–		–	
	6	–		–		Чи встановили ви угоди про взаємодопомогу з іншими країнами? *Наприклад,* діяльність правоохоронних органів, судочинство, поєднання спроможностей реагування на інциденти, спільне використання активів кібербезпеки тощо.	0	–		–	
	7	–		–		Чи підписували або ратифікували ви міжнародні договори або конвенції у сфері кібербезпеки? *Наприклад,* Міжнародний кодекс поведінки щодо інформаційної безпеки, Конвенцію про кіберзлочинність.	0	–		–	

4.2 НАСТАНОВИ ЩОДО ВИКОРИСТАННЯ КЕРІВНИЦТВА З ОЦІНКИ

Цей розділ має за мету надати країнам-членам деякі настанови та рекомендацій щодо процедур розгортання керівництва та заповнення анкети. Рекомендації, перелічені нижче, переважно випливають із відгуків, отриманих під час співбесід з представниками країн-членів:

- **Передбачити координаційну діяльність щодо збору та консолідації даних.** Більшість країн-членів визнають, що виконання такого комплексу заходів із самооцінки повинне зайняти близько 15 людино-днів. Для здійснення самооцінки доведеться звернутися до широкого кола різних зацікавлених осіб. Тому рекомендується виділити час на підготовчий етап для виявлення всіх відповідних зацікавлених осіб у державних органах, державних установах і приватному секторі.
- **Визначити центральний орган, відповідальний за проведення самооцінки на національному рівні.** Оскільки збір матеріалів для всіх показників КОНС може залучати багато зацікавлених осіб, рекомендується мати центральний орган або відомство, якому буде доручено проводити самооцінку шляхом встановлення зв'язку та координації з усіма відповідними зацікавленими особами.
- **Використовуйте проведення оцінки як спосіб обміну інформацією та спілкування на теми кібербезпеки.** Надбаний досвід, яким обмінюються країни-члени, показав, що дискусії (незалежно від того, чи проходять вони у форматі індивідуальних співбесід чи колективних семінарів) — це хороша можливість для сприяння діалогу навколо тем кібербезпеки та обміну спільними поглядами та напрямами вдосконалення. Крім того, аби засвітити ключові досягнення, обмін результатами також може сприяти просуванню тем з кібербезпеки.
- **Використовуйте Національну стратегію кібербезпеки як сферу для вибору цілей, що підлягають оцінці.** 17 цілей, що складають КОНС, були розроблені на основі цілей, які зазвичай охоплені країнами-членами в їх національних стратегіях кібербезпеки. Цілі, що охоплені як частина Національної стратегії кібербезпеки, слід використовувати як засіб для визначення обсягу оцінки. Однак Національна стратегія кібербезпеки не повинна обмежувати оцінку. Оскільки Національна стратегія кібербезпеки природно зосереджується на пріоритетах, певні сфери навмисно опускаються з Національної стратегії кібербезпеки. Однак це не означає, що така спроможність відсутня. Наприклад, у випадку, коли конкретна ціль випущена з Національної стратегії кібербезпеки, але країна має спроможності кібербезпеки, пов'язані з цією ціллю, може відбуватися оцінка цієї цілі.
- **Коли сфера дії Національної стратегії кібербезпеки розширюється, переконайтеся, що тлумачення** балів **залишається узгодженим з процесом розширення Національної стратегії кібербезпеки.** Життєвий цикл Національної стратегії кібербезпеки — це багаторічний процес. Національна стратегія кібербезпеки в деяких країнах-членах зазвичай впроваджується в дію за допомогою дорожньої карти на період від 3 до 5 років зі змінами у сфері дій між двома послідовними версіями Національної стратегії кібербезпеки. З цього погляду слід дотримуватися особливої обережності при поданні результатів самооцінки між двома версіями Національної стратегії кібербезпеки: зміни сфери дії дійсно можуть вплинути на остаточний бал зрілості. Рекомендується порівнювати бали за повним обсягом стратегічних цілей від одного року до іншого (*тобто* сукупний загальний бал).

Нагадування про механізм нарахування балів — приклад про коефіцієнт охоплення
Механізм нарахування балів передбачає два рівні балів:
(i) **сукупний загальний коефіцієнт охоплення** на основі повного переліку стратегічних цілей, присутніх у керівництві з самооцінки; і
(II) **сукупний конкретний коефіцієнт охоплення** на основі стратегічних цілей, обраних країною-членом (зазвичай відповідає цілям, наявним у Національній стратегії кібербезпеки конкретної країни).

Як попередньо встановлено (див. розділ 3.1 щодо механізму нарахування балів), сукупний конкретний коефіцієнт охоплення буде рівним або вищим за сукупний загальний коефіцієнт охоплення, оскільки останній може включати цілі, які не охоплені країною-членом, таким чином знижуючи сукупний загальний коефіцієнт охоплення. Коли країна-член додає нову ціль, сукупний коефіцієнт охоплення збільшиться (тобто охоплюється більше показників зрілості), тоді як сукупна конкретна зрілість може зменшитися (у випадку, якщо додана ціль перебуває на початковій стадії та, отже, має низький рівень зрілості).

- **Заповнюючи анкету самооцінки, майте на увазі, що основною метою є підтримка країн-членів у розбудові спроможностей кібербезпеки.** Тому під час заповнення анкети самооцінки, навіть якщо в деяких ситуаціях може бути важко відповісти на запитання точно, рекомендується вибрати відповідь, яка є найбільш загальноприйнятою. Наприклад, якщо відповідь на запитання — "ТАК" у певній сфері, але "НІ" — в іншій, країнам-членам слід пам'ятати, що відповідь "НІ" вимагає дії: або план відновлювальних заходів, або план дій щодо вдосконалення сфери, які слід враховувати при подальших розробках.

5. НАСТУПНІ КРОКИ

5.1 МАЙБУТНІ УДОСКОНАЛЕННЯ

Під час співбесід з представниками країн-членів та на етапі кабінетного дослідження були також визначені такі рекомендації щодо вдосконалення чинного Керівництва з оцінки національних спроможностей як сфери потенційного майбутнього розвитку.

- **Розробити систему нарахування балів з метою забезпечення більшої точності.** Наприклад, замість альтернативної відповіді "ТАК"/"НІ" можна було б ввести відсоток охоплення, аби краще врахувати складність консолідації спроможностей на національному рівні. Під час першого кроку було обрано простий підхід із відповідями "ТАК"/"НІ".
- **Запровадити кількісні метрики для вимірювання ефективності** національних стратегій кібербезпеки **країн-членів.** Насправді Керівництво з оцінки національних спроможностей зосереджене на оцінюванні рівня зрілості спроможностей кібербезпеки країн-членів. Це може бути доповнене метриками для вимірювання ефективності діяльності та планів дій, що реалізуються країнами-членами для розбудови цих спроможностей. Не представляється реалістичним розробити такі метрики ефективності на поточному етапі, враховуючи те, що існує невелика кількість відгуків у цій сфері, є складнощі з пошуком значущих показників, що пов'язують результат із впровадженням Національної стратегії кібербезпеки, та складнощі з розробкою реалістичних показників, які згодом можна зібрати. Однак це залишається темою для подальшої роботи.
- **Перехід від проведення самооцінки до підходу з оцінювання.** Потенційним розвитком цього керівництва в майбутньому може стати перехід до підходу з оцінювання з метою більш послідовної оцінки зрілості спроможностей кібербезпеки країн-членів. Забезпечення проведення оцінки третьою стороною могло б справді дозволити мінімізувати потенційні упередження.

ДОДАТОК А — ОГЛЯД РЕЗУЛЬТАТІВ КАБІНЕТНОГО ДОСЛІДЖЕННЯ

Додаток А містить короткий виклад попередньої роботи ENISA щодо Національної стратегії кібербезпеки та аналіз відповідних загальнодоступних моделей зрілості щодо спроможностей кібербезпеки. Зазначені нижче припущення враховуються при виборі та аналізі моделей.

- Не всі моделі базуються на ретельній методології дослідження.
- Структура та результати моделей не завжди ґрунтовно пояснюються чіткими зв'язками між різними елементами, що характеризують кожну модель.
- Деякі моделі не містять деталей щодо процесу розробки, структури та методології оцінки.
- Інші моделі та інструменти, які ми виявили, не містять жодних деталей щодо структури та змісту, а тому їх немає в переліку.
- Вибір моделей для аналізу базується на географічному охопленні. Основна увага буде приділятися моделям зрілості щодо спроможностей кібербезпеки, створеним для оцінки ефективності функціонування європейських країн. Однак важливо розширити географічне охоплення, аби проаналізувати передові практики розробки моделей зрілості в усьому світі.

Цей систематичний аналіз відповідних загальнодоступних моделей зрілості щодо спроможностей кібербезпеки був проведений з використанням спеціального керівництва з аналізу, заснованого на методології, визначеній Беккером для розробки моделей зрілості[22]. Для кожної наявної моделі зрілості було проаналізовано такі елементи, як:

- **назва моделі зрілості:** назва моделі зрілості та основні посилання;
- **первинна установа:** установа, державна чи приватна, відповідальна за розробку моделі;
- **загальна мета та ціль:** загальна сфера дії моделі та заплановані цілі;
- **кількість та визначення рівнів:** кількість рівнів зрілості моделі, а також їх загальний опис;
- **кількість та назва атрибутів:** кількість та назва атрибутів, які використовує модель зрілості. Аналіз атрибутів має трирівневу ціль:
  - розкласти модель зрілості на легко зрозумілі розділи;
  - поєднати кілька атрибутів у кластери атрибутів, що відповідають тій самій меті;
  - та надати різні погляди на предмет рівня зрілості;
- **метод оцінки:** метод оцінки моделі зрілості;
- **представлення результатів:** визначення методу візуалізації для результатів моделі зрілості. Логіка цього кроку полягає в тому, що моделі зрілості здебільшого зазнають невдачі, якщо вони занадто складні, а отже, спосіб представлення повинен відповідати практичним потребам.

[22] J. Becker, R. Knackstedt, and J. Pöppelbuß, "Developing Maturity Models for IT Management: A Procedure Model and its Application," Business & Information Systems Engineering, vol. 1, no. 3, pp. 213–222, Jun. 2009.

ПОПЕРЕДНЯ РОБОТА НАД НАЦІОНАЛЬНОЮ СТРАТЕГІЄЮ КІБЕРБЕЗПЕКИ

2012 року ENISA опублікувало два документи на тему національних стратегій кібербезпеки як частину своїх перших доробків. По-перше, у «Практичному посібнику з проведення етапів розробки та виконання Національної стратегії кібербезпеки» [23] запропоновано набір конкретних дій для ефективної реалізації Національної стратегії кібербезпеки та представлено життєвий цикл Національної стратегії кібербезпеки на чотирьох етапах: розробка стратегії, виконання стратегії, оцінка стратегії та підтримка реалізації стратегії. По-друге, у документі під назвою "Встановлення курсу національних зусиль щодо зміцнення безпеки в кіберпросторі"[24] окреслено стан стратегій кібербезпеки в ЄС та за його межами у 2012 році та запропоновано країнам-членам обов'язково визначити спільні теми та відмінності між своїми національними стратегіями кібербезпеки.

2014 року було опубліковане перше Керівництво ENISA для оцінки Національної стратегії кібербезпеки країни-члена[25]. Це Керівництво містить рекомендації та корисний досвід, а також набір інструментів розбудови спроможностей для оцінки Національної стратегії кібербезпеки (*наприклад*, визначені цілі, вхідні дані, результати, ключові показники ефективності тощо). Ці інструменти пристосовані до різних потреб країн на різних рівнях зрілості в їх стратегічному плануванні. Того ж року ENISA опублікувала «Інтерактивну онлайн мапу Національної стратегії кібербезпеки»[26], яка дозволяє користувачам швидко проконсультуватися з Національними стратегіями кібербезпеки усіх країн-членів і країн ЄАВТ, у тому числі з їх стратегічними цілями та гарними прикладами впровадження. Створена спочатку як інформаційний архів національних стратегій кібербезпеки (2014), вона в 2018 році була доповнена прикладами впровадження, а вже з 2019 року мапа виступає як *інформаційний хаб* для централізації даних, наданих країнами-членами щодо їх зусиль, направлених на підвищення національної кібербезпеки.

Опубліковане 2016 року "Керівництво з належної практики впровадження Національної стратегії кібербезпеки"[27] визначає п'ятнадцять стратегічних цілей. У цьому посібнику також аналізується стан впровадження Національної стратегії кібербезпеки в кожній країні-члені та визначаються різні прогалини та виклики щодо такого впровадження.

2018 року ENISA опублікувало "Інструмент оцінки національної стратегії кібербезпеки"[28]: інтерактивний інструмент для самооцінки, який допомагає країнам-членам оцінювати свої стратегічні пріоритети та цілі, пов'язані з їх національними стратегіями кібербезпеки. За допомогою набору простих запитань цей інструмент надає країнам-членам конкретні рекомендації щодо реалізації кожної цілі. І нарешті, "Корисний досвід інноваційної діяльності в галузі кібербезпеки в рамках Національної стратегії кібербезпеки"[29], опублікований у 2019 році, представляє тему інновацій у галузі кібербезпеки відповідно до Національної стратегії кібербезпеки. У документі викладено виклики та корисний досвід у розрізі різних інноваційних вимірів, як їх сприймають експерти цієї галузі, з метою допомогти розробці майбутніх стратегічних інноваційних цілей.

A.1 Модель зрілості спроможностей кібербезпеки для держав (CMM)

Модель зрілості спроможностей кібербезпеки для держав (CMM) була розроблена Центром глобальних спроможностей кібербезпеки (Центром розвитку спроможностей), підрозділом Оксфордської школи Мартіна при Оксфордському університеті. Мета Центру розвитку спроможностей — збільшити масштаби та ефективність розбудови спроможностей кібербезпеки як у Великобританії, так і на міжнародному рівні шляхом розгортання Моделі зрілості спроможностей кібербезпеки (CMM). Модель CMM безпосередньо націлена на країни, які бажають збільшити свої національні спроможності кібербезпеки. Вперше застосована у 2014 році, модель CMM була переглянута 2016 року після використання її в аналізі 11 національних спроможностей кібербезпеки.

[23] Національна стратегія кібербезпеки: практичний посібник з розробки та виконання (ENISA, 2012) https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] Національна стратегія кібербезпеки: встановлення курсу національних зусиль щодо зміцнення безпеки в кіберпросторі (ENISA, 2012) https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] Керівництво з оцінювання для Національної стратегії кібербезпеки (ENISA, 2014) https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] Національні стратегії кібербезпеки — інтерактивна мапа (ENISA, 2014, оновлено у 2019 році) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Цей документ вносить правки до посібника за 2012 рік: Керівництво з належної практики впровадження Національної стратегії кібербезпеки: розробка та впровадження національних стратегій кібербезпеки (ENISA, 2016) https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] Інструмент оцінки Національної стратегії кібербезпеки (2018) https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

Атрибути/виміри

Модель CMM розглядає спроможність кібербезпеки, що складається з **п'яти вимірів**, що представляють кластери спроможностей кібербезпеки. Кожен кластер являє собою інший дослідницький «об'єктив», через який можна вивчати та зрозуміти спроможності кібербезпеки. У межах п'яти вимірів **фактори** описують деталі володіння спроможностями кібербезпеки. Ці деталі є елементами, які сприяють підвищенню зрілості спроможностей кібербезпеки в кожному вимірі. Для кожного фактора кілька **аспектів** представляють його різні компоненти. Аспекти представляють організаційний метод з метою поділу показників на менші кластери, які легше осягнути. Потім кожен аспект оцінюється за допомогою **показників** з метою опису кроків, дії або структурних елементів, які вказують на конкретний етап зрілості (визначений у наступному розділі) в межах окремого аспекту, фактора та виміру.

Терміни, згадані вище, можна розкласти на рівні, як показано на рисунку нижче.

Рисунок 4. Приклад показників моделі CMM

Нижче детально описані п'ять вимірів:

i. Винайдення політики та стратегії кібербезпеки (6 факторів)
ii. Заохочення відповідальної культури кібербезпеки в суспільстві (5 факторів)
iii. Розвиток знань з кібербезпеки (3 фактори)
iv. Створення ефективного нормативно-правового регулювання (3 фактори)
v. Контроль ризиків за допомогою стандартів, організацій та технологій (7 факторів)

Рівні зрілості

Модель CMM використовує **5 рівнів зрілості**, аби визначити, наскільки країна досягла прогресу стосовно певного фактора/аспекту спроможності кібербезпеки. Ці рівні слугують миттєвим знімком наявних спроможностей кібербезпеки.

- **Запуск**: на цьому етапі або не існує зрілості кібербезпеки, або вона має дуже ембріональний характер. Можливо, були початкові дискусії щодо розбудови спроможностей кібербезпеки, але конкретних дій не було вчинено. На цьому етапі відсутні помітні докази.
- **Творення**: почали зростати та формуватися деякі особливості аспектів, але можуть бути ситуативними, дезорганізованими, погано визначеними або просто "новими". Однак докази цієї діяльності можна наочно продемонструвати.
- **Встановлення**: запроваджені та працюють елементи аспекту. Однак немає добре продуманого розгляду відповідного розподілу ресурсів. Було прийнято мало компромісних рішень щодо "відповідних" інвестицій у різні елементи аспекту. Однак аспект функціональний і визначений.

- **Стратегічний**: було зроблено вибір щодо того, які частини аспекту є важливими, а які менш важливими для конкретної організації чи країни. Стратегічний етап відображає той факт, що цей вибір був зроблений залежно від конкретних обставин країни або організації.
- **Динамічний**: на цьому етапі запроваджені чіткі механізми зміни стратегії залежно від переважних обставин, таких як технологія середовища загрози, глобальний конфлікт або суттєві зміни в одній зі сфер, яка розглядається (*наприклад,* кіберзлочинність або конфіденційність/приватність). Динамічні організації розробили методи поступової зміни стратегій. Швидке прийняття рішень, перерозподіл ресурсів та постійна увага до мінливого середовища є особливостями цього етапу.

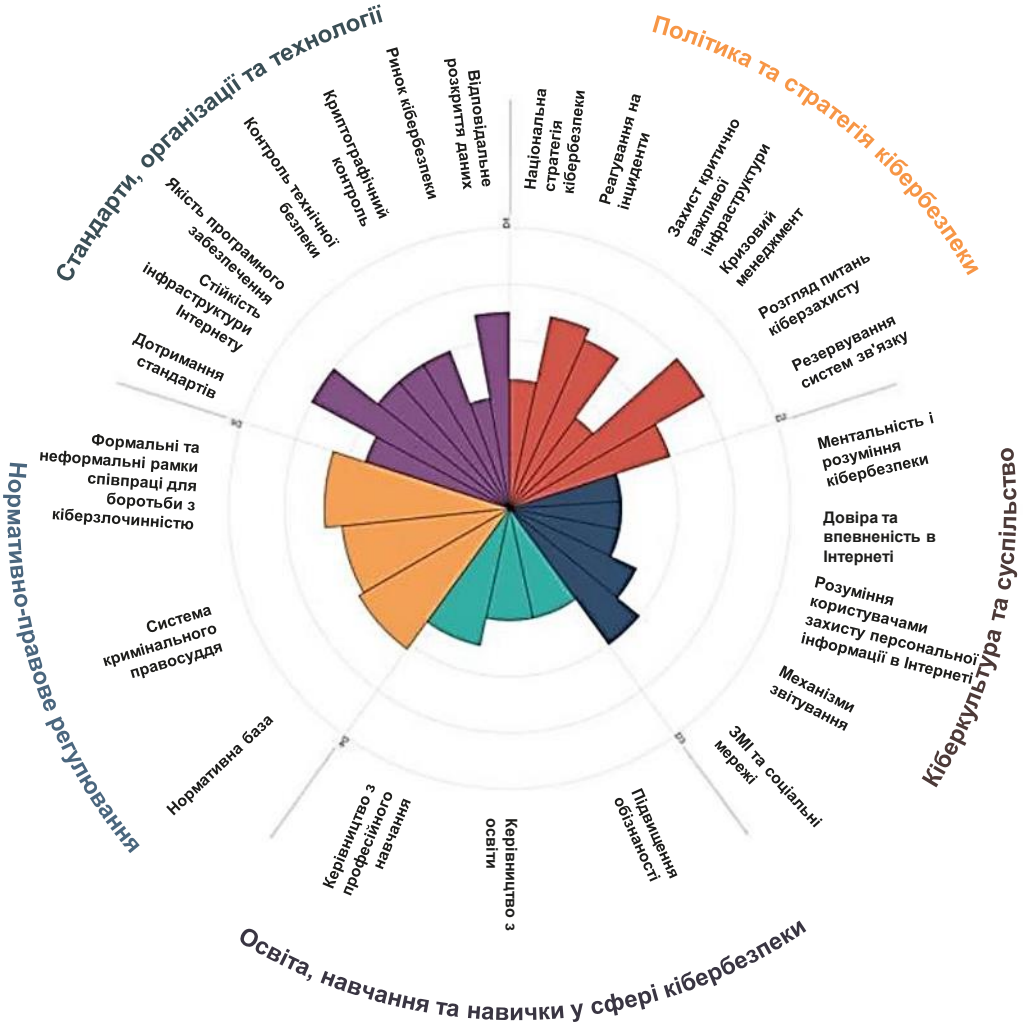
Метод оцінки

Оскільки Центр розвитку спроможностей не має ретельного та глибокого розуміння кожного внутрішнього контексту, в якому застосовується модель, він працює разом із міжнародними організаціями, приймаючими міністерствами або організаціями у відповідній країні з метою аналізу зрілості спроможностей кібербезпеки. Для того щоб оцінити рівень зрілості п'яти вимірів, включених до моделі CMM, Центр розвитку спроможностей та приймаюча організація зустрічаються з відповідними національними зацікавленими особами державного та приватного секторів протягом 2 або 3 днів з метою проведення фокус-груп щодо вимірів у рамках моделі CMM. Кожен вимір обговорюється принаймні двічі різними кластерами зацікавлених осіб. Це становить попередній пул даних для подальшої оцінки.

Спосіб або представлення результатів

Модель CMM забезпечує огляд рівня зрілості кожної країни за допомогою радара, що складається з п'яти розділів, по одному для кожного виміру. Кожен вимір являє собою п'яту частину графіка, причому п'ять стадій зрілості для кожного фактора простягаються назовні від центру графіка; як показано нижче, "запуск" перебуває найближче до центру графіка, а "динамічний" — на периметрі.

Рисунок 5. Модель CMM: огляд результатів



Центр глобальних спроможностей кібербезпеки Оксфордської школи Мартіна, Оксфордський університет, 2017.

A.2 Модель зрілості спроможностей кібербезпеки (C2M2)

Модель зрілості спроможностей кібербезпеки (C2M2) була розроблена Міністерством енергетики США у співпраці з експертами приватного та державного секторів. Метою Центру розвитку спроможностей є допомога організаціям усіх секторів, типів та розмірів в оцінці та вдосконаленні своїх програм з кібербезпеки та зміцненні їх експлуатаційної стійкості. Модель C2M2 фокусується на впровадженні та управлінні практикою кібербезпеки, пов'язаною з інформацією, інформаційними технологіями (IT) та активами операційних технологій (OT) і середовищами, в яких вони функціонують. Модель C2M2 визначає моделі зрілості як "сукупність характеристик, атрибутів, показників або зразків, що показують спроможності та прогрес у певній дисципліні". Вперше застосована у 2014 році, модель C2M2 була переглянута 2019 року.

Атрибути/виміри

Модель C2M2 розглядає **десять сфер**, що представляють логічне групування практик кібербезпеки. Кожен набір практик представляє діяльність, яку організація може виконувати для встановлення та розвитку спроможностей у цій сфері. Потім кожна сфера асоціюється з **унікальною ціллю управління та кількома цілями підходу.** У рамках як підходу, так і цілей управління деталізовані **кілька практик** для опису відомчої діяльності.

Зв'язок між цими поняттями підсумовано нижче.

Рисунок 6. Приклад індикатора моделі C2M2

Нижче детально описані десять сфер:

i. Управління ризиками (РИЗИК)
ii. Управління активами, змінами та конфігурацією (АКТИВ)
iii. Управління ідентифікацією та доступом (ДОСТУП)
iv. Управління загрозами та вразливістю (ЗАГРОЗА)
v. Ситуативна обізнаність (СИТУАЦІЯ)
vi. Реагування на події та інциденти (РЕАГУВАННЯ)
vii. Управління ланцюгами постачання та зовнішніми взаємозалежностями (ВЗАЄМОЗАЛЕЖНОСТІ)
viii. Управління персоналом (ПЕРСОНАЛ)
ix. Архітектура кібербезпеки (АРХІТЕКТУРА)
x. Управління програмою кібербезпеки (ПРОГРАМА)

Рівні зрілості

Модель C2M2 використовує **4 рівні зрілості** (що називаються рівні показника зрілості або MIL) для визначення подвійного прогресу зрілості: прогрес підходу та прогрес управління. Значення MIL мають діапазон від MIL0 до MIL3 і призначені для незалежного застосування до кожної сфери.

- **MIL0:** практики не виконуються.
- **MIL1:** початкові практики виконуються, але можуть бути ситуативними.
- **MIL2:** характеристики управління:
  - практика документується;
  - для забезпечення процесу надаються належні ресурси;
  - персонал, який реалізує практику, має адекватні навички та знання; і
  - передані відповідальність та повноваження для виконання практик;

  характеристика підходу:
  - практика є повнішою або більш вдосконаленою, ніж у MIL1.
- **MIL3:** характеристики управління:
  - у діяльності керуються політикою (або іншими організаційними директивами);
  - цілі ефективності діяльності у сфері визначаються та контролюються для відстеження досягнень; і
  - задокументована практика для діяльності у сфері стандартизована та вдосконалена на всьому підприємстві;

  характеристика підходу:
  - практики є більш повними або вдосконаленими, ніж у MIL2.

Метод оцінки

Модель C2M2 призначена для використання з **методологією самооцінки** та набором інструментів (доступний за запитом) для організації з метою вимірювання та вдосконалення своєї програми з кібербезпеки. Самооцінка за допомогою набору інструментів може бути виконана за один день, але набір інструментів міг бути пристосований для більш скрупульозного процесу оцінювання. Крім того, модель C2M2 можна використовувати для керівництва розробкою нової програми з кібербезпеки.

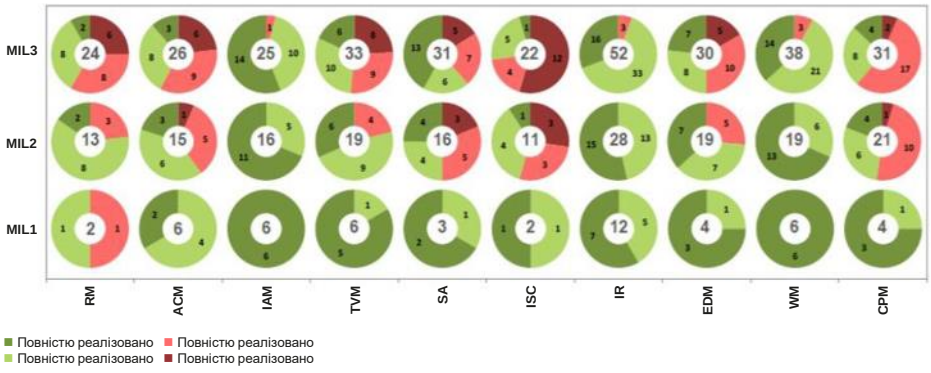
Зміст моделі представлений на високому рівні абстракції, тому його можуть інтерпретувати організації різних типів, структур, розмірів і галузей. Широке використання моделі будь-яким сектором може підтримати оцінку ефективності спроможностей кібербезпеки такого сектору.

Спосіб або представлення результатів

Модель C2M2 надає звіт про бали оцінювання, сформований на основі результатів дослідження. У звіті представлені результати двох оглядів: огляд цілі, який показує відповіді на практичні запитання в розрізі кожної сфери та її цілей, і огляд сфери, який показує відповіді в розрізі всіх сфер та рівнів MIL. Обидва огляди базуються на системі представлення, що подається у вигляді кругових діаграм (або «кільцевих діаграм»), одна діаграма на відповідь, та за допомогою механізму нарахування балів за системою світлофора. Як показано на рисунку 7, червоні сектори на кільцевій діаграмі показують рахунок кількості запитань, на які під час опитування надана відповідь: "Не реалізовано" (темно-червоний) або "Частково реалізовано" (світло-червоний). Зелені сектори показують кількість запитань, на які було отримано відповіді "Значною мірою реалізовано" (світло-зелений) або "Повністю реалізовано" (темно-зелений).

Рисунок 7 нижче є прикладом картки нарахування балів в кінці оцінки зрілості. По осі X розташовані 10 сфер моделі C2M2, а по осі Y — рівні зрілості (MIL). Дивлячись на графік та розглядаючи сферу управління ризиками (УР), можна помітити три кругові діаграми, одна діаграма для кожного рівня зрілості ML1, ML2 та ML3. На графіку для сфери УР виокремлено, що існує два пункти, які слід оцінити для досягнення першого рівня зрілості, ML1. У цьому випадку один бал "Значною мірою реалізовано", а інший бал — "Частково реалізовано". Для другого рівня зрілості, ML2, модель передбачає оцінку 13 пунктів для оцінювання. Два з цих 13 пунктів належать до першого рівня ML1, а 11 до другого рівня — ML2. Те саме стосується і третього рівня ML3.

Рисунок 7. Модель C2M2 – Приклад огляду сфери



Джерело: Міністерство енергетики США, Управління електропостачання та енергетичної надійності, 2015.

A.3 Керівництво для удосконалення кібербезпеки критично важливої інфраструктури

Керівництво для удосконалення кібербезпеки критично важливої інфраструктури було розроблене в рамках Національного інституту стандартів і технологій (НІСТ). Воно зосереджене на керівництві діяльністю в галузі кібербезпеки та управлінні ризиками в організації. Воно орієнтоване на всі типи організацій, незалежно від розміру, ступеня ризику кібербезпеки або ступеня складності кібербезпеки. Оскільки це керівництво, а не модель, то воно побудоване інакше, ніж проаналізовані вище моделі.

Керівництво складається з трьох частин: це базова частина Керівництва, яруси впровадження та профілі Керівництва:

- **Базова частина Керівництва** — набір дій з кібербезпеки, бажаних результатів та застосовних посилань, які є загальними для секторів критичної інфраструктури. Вони подібні до атрибутів або вимірів, що зустрічаються в моделях зрілості спроможностей кібербезпеки.
- **Яруси впровадження Керівництва** ("яруси") дають контекст того, як організація розглядає ризик кібербезпеки та запроваджені процеси управління цим ризиком. Маючи шкалу від частковий (ярус 1) до адаптивний (ярус 4), яруси описують зростання ступеню суворості та складності в практиці управління ризиками кібербезпеки. Яруси не репрезентують рівні зрілості, вони, швидше за все, призначені для підтримки процесу прийняття організаційних рішень про те, як управляти ризиком кібербезпеки, а також про те, які виміри організації є більш пріоритетними та можуть отримати додаткові ресурси.
- **Профіль Керівництва** ("профіль") представляє кінцеві результати, засновані на потребах бізнесу, які організація обрала з категорій та підкатегорій Керівництва. Профіль можна охарактеризувати з урахуванням узгодження стандартів, настанов і практики з базовою частиною Керівництва в конкретному сценарії впровадження. Профілі можна використовувати для виявлення можливостей вдосконалення стану кібербезпеки, порівнюючи профіль "Поточний" (стан "як є") із профілем "Ціль" (стан "має бути").

Базова частина Керівництва

Базова частина Керівництва складається з п'яти **функцій**. Якщо розглядати їх разом, ці функції забезпечують стратегічний погляд високого рівня на життєвий цикл управління ризиками кібербезпеки в організації. Крім того, базова частина Керівництва визначає основні ключові **категорії** та **підкатегорії** для кожної функції та узгоджує їх із прикладами інформативних посилань, такими як наявні стандарти, настанови та практику для кожної підкатегорії.

Нижче детально описано функції та категорії.

i. **Визначити**: сформуйте організаційне розуміння того, як керувати ризиками кібербезпеки для систем, людей, активів, даних і спроможностей.
   - Підкатегорії: управління активами, бізнес-середовище, управління, оцінка ризику та стратегія управління ризиками.

ii. **Захистити**: розробити та впровадити відповідні запобіжні заходи для забезпечення надання критично важливих сервісів.
   - Підкатегорії: управління ідентифікацією та контроль доступу, обізнаність та навчання, безпека даних, процеси та процедури захисту інформації, підтримка реалізації та технологія захисту.

iii. **Виявити**: розробити та впровадити відповідні заходи для визначення події кібербезпеки.
   - Підкатегорії: аномалії та події, безперервний моніторинг безпеки та процеси виявлення.

iv. **Зреагувати**: розробити та впровадити відповідні заходи для вжиття заходів стосовно виявленого інциденту кібербезпеки.
   - Підкатегорії: планування реагування, комунікації, аналіз, пом'якшення наслідків та вдосконалення.

v. **Відновити**: розробити та впровадити відповідні заходи для реалізації планів щодо відновлення функціонування системи та для відновлення будь-яких спроможностей або сервісів, які були порушені внаслідок інциденту з кібербезпекою.
   - Підкатегорії: планування відновлення, вдосконалення та комунікації.

Рисунок 8. Приклад з Керівництва для удосконалення кібербезпеки критично важливої інфраструктури

Яруси

Керівництво для удосконалення кібербезпеки критично важливої інфраструктури спирається на **4 яруси**, кожен з яких визначається за трьома осями: процес управління ризиками, програма інтегрованого управління ризиками та зовнішня участь. Яруси не слід розглядати як рівні зрілості, а як керівництво, яка надає організаціям контекстуалізацію їх поглядів на ризик кібербезпеки та запроваджені процеси управління цим ризиком.

- **Ярус 1: частковий**
  - **Процес управління ризиками**: організаційна практика управління ризиками кібербезпеки не формалізовані, а управління ризиками здійснюється ситуативно, а іноді у формі реагування після виникнення.
  - **Програма інтегрованого управління ризиками**: на організаційному рівні обмежена поінформованість щодо ризику кібербезпеки. Організація впроваджує управління ризиками кібербезпеки нерегулярно, в кожному конкретному випадку, і може не мати процесів, які дозволяють обмінюватися інформацією про кібербезпеку всередині організації;
  - **Зовнішня участь**: організація не розуміє своєї ролі в більшій екосистемі стосовно ні її взаємозалежностей, ні підлеглих. Організація здебільшого не обізнана про кіберризики ланцюга постачання продуктів і сервісів, які вона надає, і які вона використовує.
- **Ярус 2: ризик-орієнтований**
  - **Процес управління ризиками**: практика управління ризиками затверджується керівництвом, але можуть бути не запроваджені як політика в діяльності всієї організації.
  - **Програма інтегрованого управління ризиками**: є поінформованість щодо ризику кібербезпеки на організаційному рівні, проте загальний організаційний підхід до управління ризиком кібербезпеки не запроваджений. Оцінка кібер-ризику організаційних та зовнішніх активів відбувається, але зазвичай не є багаторазовою або повторюваною.
  - **Зовнішня участь**: загалом організація розуміє свою роль у більшій екосистемі стосовно власних взаємозалежностей або підлеглих, але не обох категорій. Крім того, організація усвідомлює кіберризики ланцюга постачання, пов'язані з продуктами та сервісами, які вона надає та використовує, але щодо цих ризиків вона не діє послідовно або офіційно.
- **Ярус 3: багаторазовий**
  - **Процес управління ризиками**: практика управління ризиками офіційно затверджена в організації та виражається як політика. Організаційна практика кібербезпеки регулярно оновлюється на основі застосування процесів управління ризиками до змін у вимогах господарської діяльності/завдань, мінливих загроз і технологічного середовища.
  - **Програма інтегрованого управління ризиками**: на рівні організації є підхід до управління ризиками кібербезпеки. Визначені, впроваджуються за призначенням та переглядаються ризик-орієнтовані політики, процеси та процедури. Старше керівництво забезпечує врахування кібербезпеки на всіх напрямах діяльності в організації.

- Зовнішня участь: організація розуміє свою роль, взаємозалежності та підлеглих у більшій екосистемі та може сприяти ширшому розумінню громадою ризиків. Організація поінформована про кіберризики ланцюга постачання, пов'язані з продуктами та сервісами, які вона надає і які вона використовує.

- **Ярус 4: адаптивний**
  - **Процес управління ризиками:** організація адаптує свою практику кібербезпеки на основі попередньої та поточної діяльності з кібербезпеки, в тому числі на основі набутого досвіду та прогнозних показників.
  - **Програма інтегрованого управління ризиками**: є загально-організаційний підхід до управління ризиками кібербезпеки, який використовує ризик-орієнтовану політику, процеси та процедури для вирішення потенційних подій кібербезпеки.
  - **Зовнішня участь:** організація розуміє свою роль, взаємозалежності та підлеглих у більшій екосистемі та сприяє ширшому розумінню громадою ризиків.

Метод оцінки

Керівництво для удосконалення кібербезпеки критично важливої інфраструктури призначене для організацій, які самостійно оцінюють свій ризик, аби зробити свій підхід до кібербезпеки та інвестиції більш раціональним, ефективним та цінним. З метою вивчення ефективності інвестицій, організація повинна спочатку чітко зрозуміти свої організаційні цілі, взаємозв'язок між цими цілями та підтримувальними кінцевими результатами кібербезпеки. Кінцеві результати кібербезпеки базової частини Керівництва підтримують процес проведення самооцінки щодо ефективності інвестицій та діяльності з кібербезпеки.

A.4 Катарська модель зрілості спроможностей кібербезпеки (Q-C2M2)

Катарська модель зрілості спроможностей кібербезпеки (Q-C2M2) була розроблена юридичним факультетом Катарського університету в 2018 році. Модель Q-C2M2 базується на різних наявних моделях для побудови комплексної методології оцінки з метою вдосконалення катарської концепції кібербезпеки.

Атрибути/виміри

Модель Q-C2M2 застосовує підхід з Керівництва Національного інституту стандартів і технологій (HICT), який використовує п'ять основних функцій як основні сфери моделі. П'ять основних функцій застосовні в катарському контексті, оскільки вони є загальними для критично важливих секторів інфраструктури, що є важливим елементом катарської концепції кібербезпеки. Модель Q-C2M2 базується на **п'яти сферах**, а кожна сфера при цьому розділена на кілька **підсфер**, аби охопити весь спектр зрілості спроможностей кібербезпеки.

Нижче детально описані п'ять сфер.

i. **Сфера "Зрозуміти"** включає чотири підсфери: кіберуправління, активи, ризики та навчання.
ii. Підсфери **у сфері "Гарантувати"** включають захист даних, безпеку технологій, безпеку контролю доступу, безпеку комунікацій та безпеку персоналу.
iii. **Сфера "Викривати"** включає моніторинг, управління інцидентами, виявлення, аналіз та викриття.
iv. **Сфера "Реагувати"** включає планування реагування, пом'якшення наслідків та комунікацію при реагуванні.
v. **Сфера "Підтримувати"** включає планування відновлення, управління цілісністю процесу, вдосконалення та зовнішні взаємозалежності.

Рівні зрілості

Модель Q-C2M2 використовує **5 рівнів зрілості,** вимірюючи зрілість спроможності державного суб'єкта або недержавної організації на рівні основної функції. Ці рівні спрямовані на оцінку зрілості у п'яти сферах, детально описаних у попередньому розділі.

- **Ініціювання**: використовує спеціальні практики та процеси кібербезпеки в межах деяких сфер.
- **Впровадження**: ухвалені політики щодо впровадження всіх заходів з кібербезпеки в межах сфер з метою завершення реалізації в певний час.
- **Розробка**: впроваджені політики та практика для розвитку і вдосконалення діяльності з кібербезпеки в межах сфер з метою запропонувати нові заходи для реалізації.
- **Адаптація**: інспектується і переглядається діяльність з кібербезпеки та адаптується практика на основі прогнозних показників, отриманих із попереднього досвіду та заходів.
- **Гнучкість**: продовжує практикувати адаптаційний етап із додатковим акцентом на гнучкість і швидкість під час реалізації діяльності у сферах.

Метод оцінки

Модель Q-C2M2 перебуває на початковій стадії досліджень і ще не розроблена для впровадження. Це концепція, яка може бути використана для розгортання детальної моделі оцінки для катарських організацій у майбутньому.

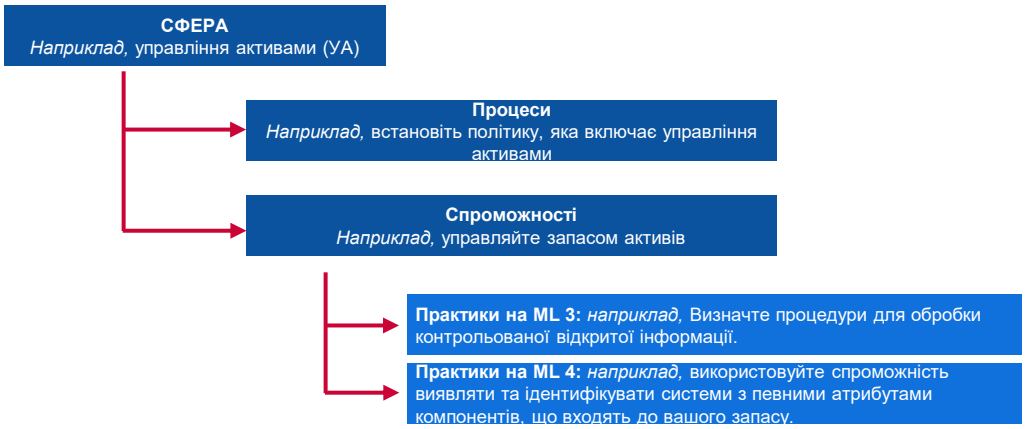
A.5 Сертифікація моделі зрілості кібербезпеки (CMMC)

Сертифікація моделі зрілості кібербезпеки (CMMC) була розроблена Міністерством оборони США (DoD) у співпраці з Університетом Карнегі — Меллона та Лабораторією прикладної фізики Університету Джона Хопкінса. Основною ціллю Міністерства оборони в розробці цієї моделі є захист інформації від сектору оборонної промислової бази (DIB). Інформація, на яку націлений стандарт CMMC, класифікується як "інформація федерального уряду" — інформація, що надається урядом або створюється для нього за контрактом і не призначена для публічного оприлюднення, або як "контрольована відкрита інформація" — інформація, яка вимагає заходів захисту або контролю в разі розповсюдження відповідно до законів, нормативних актів і загальнодержавних політик. Стандарт CMMC вимірює зрілість кібербезпеки та забезпечує передові практики разом з елементом сертифікації для забезпечення впровадження практик, пов'язаних з кожним рівнем зрілості. Остання версія стандарту CMMC була випущена у 2020 році.

Атрибути/виміри

Стандарт CMMC розглядає **сімнадцять сфер,** що представляють кластери процесів і спроможностей кібербезпеки. Потім кожна сфера розділяється на кілька **процесів**, подібних у межах різних сфер; і на від однієї до багатьох **спроможностей**, що охоплюють п'ять рівнів зрілості. При цьому спроможності (або спроможність) детально описуються в **практиках** для кожного відповідного рівня зрілості.

Зв'язок між цими поняттями полягає в такому:
Рисунок 9. Приклад показників стандарту CMMC



Нижче детально описано сімнадцять сфер:

i. Контроль доступу (КД)
ii. Управління активами (УА)
iii. Аудит та підзвітність (АП)
iv. Обізнаність та навчання (ОН)
v. Управління конфігураціями (УК)
vi. Ідентифікація та автентифікація (ІА)
vii. Реагування на інциденти (РІ)
viii. Підтримка реалізації (ПР)
ix. Медіа захист (МЗ)
x. Безпека персоналу (БП)
xi. Фізичний захист (ФЗ)
xii. Відновлення роботи (ВР)
xiii. Управління ризиками (УР)
xiv. Оцінка безпеки (ОБ)
xv. Ситуативна обізнаність (СО)
xvi. Захист системи та комунікацій (СК)
xvii. Цілісність системи та інформації (СІ)

Рівні зрілості

Стандарт CMMC використовує **5 рівнів зрілості**, визначених на основі процесів і практик. Для того щоб досягти певного рівня зрілості у стандарті CMMC, організація повинна виконати передумови для процесів і практик для цього самого рівня. Це також передбачає виконання передумов усіх рівнів, що перебувають нижче цього рівня.

Рисунок 10. Рівні зрілості стандарту CMMC

- **Рівень 1**
  - **Процеси — виконуються**: оскільки організація може лише виконувати ці практики нерегулярно і може покладатися або не покладатися на документацію. Зрілість процесу не оцінюється для рівня 1.
  - **Практики — базова кібергігієна:** рівень 1 фокусується на захисті інформації FCI (інформація федерального уряду) і складається лише з практик, які відповідають основним вимогам захисту.
- **Рівень 2**
  - **Процеси — задокументовані:** рівень 2 вимагає, аби організація встановила та задокументувала практики та політики для управління процесом впровадження своїх зусиль у рамках стандарту CMMC. Документація практик дозволяє людям виконувати їх у повторюваній формі. Організації розвивають зрілі спроможності, документуючи свої процеси, а потім практикуючи їх, як задокументовано.
  - **Практики — кібергігієна середнього рівня**: рівень 2 слугує етапом просування від рівня 1 до рівня 3 і складається з підгрупи вимог безпеки, зазначених у NIST SP 800-171, а також практик з інших стандартів і джерел.

- **Рівень 3**
  - **Процеси — керований:** рівень 3 вимагає, аби організація створила, підтримувала та надавала ресурси для плану, що демонструє управління діяльністю щодо впровадження практики. План може включати інформацію про завдання, цілі, плани заходів, ресурси, необхідну підготовку та залучення відповідних зацікавлених осіб.
  - **Практики — хороша кібергігієна**: рівень 3 зосереджується на захисті контрольованої відкритої інформації та охоплює всі вимоги до безпеки, зазначені в NIST SP 800-171, а також додаткові практики з інших стандартів та джерел з метою пом'якшення загроз.
- **Рівень 4**
  - **Процеси — переглянутий**: рівень 4 вимагає, аби організація перевіряла та вимірювала практики щодо ефективності. На додаток до вимірювання практик щодо ефективності організації на цьому рівні можуть вживати коригувальних заходів, коли це необхідно, та регулярно інформувати вище керівництво про стан або проблемні питання.
  - **Практики — дуже активний**: рівень 4 зосереджений на захисті контрольованої відкритої інформації та охоплює підгрупу посилених вимог безпеки. Ці практики покращують спроможності організації виявляти та реагувати щодо спрямування уваги та адаптації до змін тактики, технік та процедур.
- **Рівень 5**
  - **Процеси — оптимізація**: рівень 5 вимагає від організації проведення стандартизації та оптимізації впровадження процесів в рамках організації.
  - **Практики — розвинений/дуже активний**: рівень 5 зосереджений на захисті контрольованої відкритої інформації. Додаткові практики збільшують глибину та складність спроможностей кібербезпеки.

Метод оцінки

CMMC — це порівняно молода модель, доопрацьована в першому кварталі 2020 року. До цього часу її ще не було впроваджено в жодній організації. Однак підрядники Міністерства оборони розраховують звернутися до сертифікованих зовнішніх експертів для проведення аудиту. Міністерство оборони очікує від своїх підрядників впровадження передових практик для сприяння кібербезпеці та захисту конфіденційної інформації.

A.6 Модель зрілості кібербезпеки громади (CCSMM)

Модель зрілості кібербезпеки громади (CCSMM) була розроблена Центром безпеки та ефективності інфраструктури Техаського університету. Мета моделі CCSMM полягає у кращому визначенні методів визначення поточного статусу громади з огляду на її кіберготовність та забезпеченні дорожньої карти для громад, яких їм слід дотримуватися у своїх підготовчих зусиллях. Громади, на які спрямована дія моделі КМКП, є переважно органами місцевого самоврядування або органами штату. Модель CCSMM була розроблена у 2007 році.

Атрибути/виміри

Рівні зрілості визначаються відповідно до **6 основних вимірів**, які охоплюють різні аспекти кібербезпеки в громадах та організаціях. Ці виміри чітко визначені для кожного рівня зрілості (детально на рисунку 31: короткий огляд моделі **CCSMM**). Ці 6 вимірів такі:

i. Загрози вирішуються
ii. Метрики
iii. Обмін інформацією
iv. Технологія
v. Навчання
vi. Тестування

Рівні зрілості

Модель CCSMM спирається на **5 рівнів зрілості**, що ґрунтуються на основних видах загроз та діяльності, які розглядаються на рівні.

- **Рівень 1: поінформованість про безпеку.** Основною темою діяльності на цьому рівні є інформування приватних осіб та організацій про загрози, проблеми та проблемні питання, пов'язані з кібербезпекою.
- **Рівень 2: рівень розвитку процесів**, призначений допомогти громадам встановити та вдосконалити процеси безпеки, необхідні для ефективного розв'язання питань кібербезпеки.
- **Рівень 3: доступна інформація.** Розроблений для вдосконалення механізмів обміну інформацією в межах громади, аби громада могла ефективно співвідносити, на перший погляд, розрізнену інформацію.
- **Рівень 4: розробка тактики.** Елементи цього рівня спроєктовані для розробки кращих та більш активних методів виявлення та реагування на атаки. До цього рівня більшість превентивних методів повинні вже бути впроваджені.
- **Рівень 5: повна операційна спроможність безпеки.** Цей рівень представляє ті елементи, які мають бути запроваджені для будь-якої організації, аби вважатися повністю оперативно готовою до вирішення будь-якого типу кіберзагрози.

Рисунок 31. Короткий огляд вимірів моделі CCSMM у розрізі рівнів

	Рівень 1 Обізнаний про безпеку	**Рівень 2** Розвиток процесу	**Рівень 3** Доступна інформація	**Рівень 4** Розвиток тактики	**Рівень 5** Повна операційна спроможність безпеки
Загрози вирішуються	Не структурований	Не структурований	Структурований	Структурований	Структури вищого ступеня
Метрики	Уряд, промисловість, громадяни	Уряд, промисловість, громадяни	Уряд, промисловість, громадяни	Уряд, промисловість, громадяни	Уряд, промисловість, громадяни
Обмін інформацією	Комітет з питань обміну інформацією	Вебсайт безпеки громади	Інформаційно-координаційний центр	Координація на рівні штату/держави	Повне бачення інформації
Технологія	Реєстри, Урядова служба оповіщення про надзвичайні ситуації, контроль доступу, шифрування	Захищений брандмауер вебсайтів, резервне копіювання	Координація подій через ПЗ СВВ/СОІ (IDS/IPS)	Цілодобові операції за участі персоналу	Автоматизовані операції
Навчання	1-денний семінар у громаді	Проведення відпрацювання кібербезпеки в громаді (CCSE)	Оцінки вразливості	Операційна безпека	Імітація міждисциплінарної атаки/вторгнення "Червоної команди"
Тестування	Темний екран — кінець перетворення	Темний екран громади	Темний екран операції	Вправа "Обмежений чорний демон"	Вправа "Чорний демон"

Метод оцінки

Модель CCSMM як методологія оцінки має застосовуватися громадами з урахуванням вхідних даних від правоохоронних органів штату та федерального рівня. Вона має на меті допомогти громаді визначити, що є найбільш важливим, які є найбільш імовірні цілі та що потрібно захищати (і якою мірою). З урахуванням цих цілей можна розробити плани щодо приведення кожного аспекту громади до необхідного рівня зрілості кібербезпеки. Особливі відомості, що генеруються моделлю CCSMM, допомагають визначити цілі різних тестів та відпрацювань, які можуть бути використані для вимірювання ефективності встановлених програм.

A.7Модель зрілості інформаційної безпеки для Керівництва NICT з кібербезпеки (ISMM)

Модель зрілості інформаційної безпеки (ISMM) була розроблена в Коледжі комп'ютерних наук та техніки Університету нафти та корисних копалин короля Фахда в Саудівській Аравії. Вона пропонує нову модель зрілості спроможностей для вимірювання впровадження заходів з кібербезпеки. Мета моделі ISMM — дати можливість організаціям вимірювати прогрес у впровадженні з часом, регулярно використовуючи той самий інструмент вимірювання, аби забезпечити підтримку бажаного стану безпеки. Модель ISMM була розроблена 2017 року.

Атрибути/виміри

Модель ISMM спирається на наявні оцінені сфери Керівництва NIST та додає вимір щодо оцінки відповідності. У моделі охоплено **23 сфери оцінки**, аби забезпечити оцінку стану безпеки організації. 23 сфери оцінки такі:

i. управління активами,
ii. бізнес-середовище,
iii. управління,
iv. оцінка ризику,
v. стратегія управління ризиками,
vi. оцінка відповідності,
vii. контроль доступу,
viii. обізнаність та навчання,
ix. безпека даних,
x. процеси та процедури захисту інформації,
xi. підтримка реалізації,
xii. технологія захисту,
xiii. аномалії та події,
xiv. безперервний моніторинг безпеки,
xv. процеси виявлення,
xvi. планування реагування,
xvii. комунікація реагування,
xviii. аналіз реагування,
xix. пом'якшення наслідків реагування,
xx. вдосконалення реагування,
xxi. планування відновлення,
xxii. вдосконалення відновлення та
xxiii. комунікація відновлення.

Рівні зрілості

Модель ISMM спирається на **5 рівнів зрілості**, які, на жаль, не описані детально у доступній документації.

- **Рівень 1:** процес виконання.
- **Рівень 2:** процес управління.
- **Рівень 3:** процес встановлення.
- **Рівень 4:** процес передбачення.
- **Рівень5:** процес оптимізації.

Метод оцінки

Модель ISMM не пропонує жодної конкретної методології для проведення оцінки для організацій.

A.8 Модель спроможності внутрішнього аудиту (IA-CM) для державного сектору

Модель спроможності внутрішнього аудиту (IA-CM) була розроблена Інститутом внутрішніх аудиторів Фонду досліджень з метою розбудови спроможностей та адвокації шляхом самооцінки в державному секторі. Модель IA-CM орієнтована на професіоналів аудиту та надає огляд самої моделі разом із Посібником із застосування моделі, аби допомогти у використанні моделі як інструменту самооцінки.

Незважаючи на те що модель IA-CM орієнтована на спроможності внутрішнього аудиту, а не на розбудову спроможностей кібербезпеки, вона побудована як інструмент самооцінки зрілості для суб'єктів державного сектору, який можна застосовувати у всьому світі для вдосконалення процесів та ефективності. Оскільки сфера дії не зосереджена на кібербезпеці, атрибути аналізуватися не будуть. Модель IA-CM була доопрацьована у 2009 році.

Рівні зрілості

Модель спроможності внутрішнього аудиту (IA-CM) включає **5 рівнів зрілості**, кожен з яких описує характеристики та спроможності діяльності внутрішнього аудиту на цьому рівні. Рівні спроможностей у моделі забезпечують дорожню карту для постійного вдосконалення.

- **Рівень 1: початковий**
  Немає стійких, повторюваних спроможностей — залежить від індивідуальних зусиль
  - Ситуативний або неструктурований.
  - Поодинокі окремі перевірки чи аналізи документів та транзакцій на предмет точності та відповідності.
  - Результати роботи залежать від навичок конкретної особи, яка обіймає посаду.
  - Не встановлено жодної професійної практики, за винятком практики професійних асоціацій.
  - У разі потреби затвердження фінансування керівництвом.
  - Відсутність інфраструктури.
  - Аудитори, ймовірно, є частиною більшого організаційного підрозділу.
  - Інституційні спроможності не розвинені.
- **Рівень 2: інфраструктура**
  Стійкі та повторювані практики та процедури
  - Ключове питання або виклик рівня 2 полягає в тому, як встановити та підтримувати повторюваність процесів і, отже, спроможність повторюваності.
  - Встановлюються відносини звітності в рамках внутрішнього аудиту, управлінська та адміністративна інфраструктура, а також професійні практики та процеси (керівництво, процеси та процедури внутрішнього аудиту).
  - Планування аудиту, засноване головним чином на пріоритетах управління.
  - Постійна залежність, по суті, від навичок та компетенції конкретних людей.
  - Часткова відповідність стандартам.
- **Рівень 3: інтегрований**
  Управлінська та професійна практика застосовуються рівномірно
  - Політики, процеси та процедури внутрішнього аудиту визначаються, документуються та інтегруються одна в одну та в інфраструктуру організації.
  - Управління внутрішнім аудитом та професійна практика добре налагоджені та однаково застосовуються у діяльності внутрішнього аудиту.
  - Внутрішній аудит починає узгоджуватися з бізнес-діяльністю організації та ризиками, з якими вона стикається.
  - Внутрішній аудит еволюціонує від проведення лише традиційного внутрішнього аудиту до інтеграції як командного гравця та надання консультацій щодо досягнення результативності та управління ризиками.
  - Основна увага приділяється побудові команди та спроможності виконання внутрішнього аудиту, його незалежності та об’єктивності.
  - Загалом відповідає стандартам.
- **Рівень 4: керований**
  Інтегрує інформацію з усієї організації для вдосконалення управління нею та управління ризиками
  - Внутрішній аудит та очікування ключових зацікавлених осіб узгоджуються.
  - Метрики ефективності запроваджені для вимірювання та моніторингу процесів та результатів внутрішнього аудиту.
  - Внутрішній аудит визнаний таким, що вносить значний внесок в організацію.

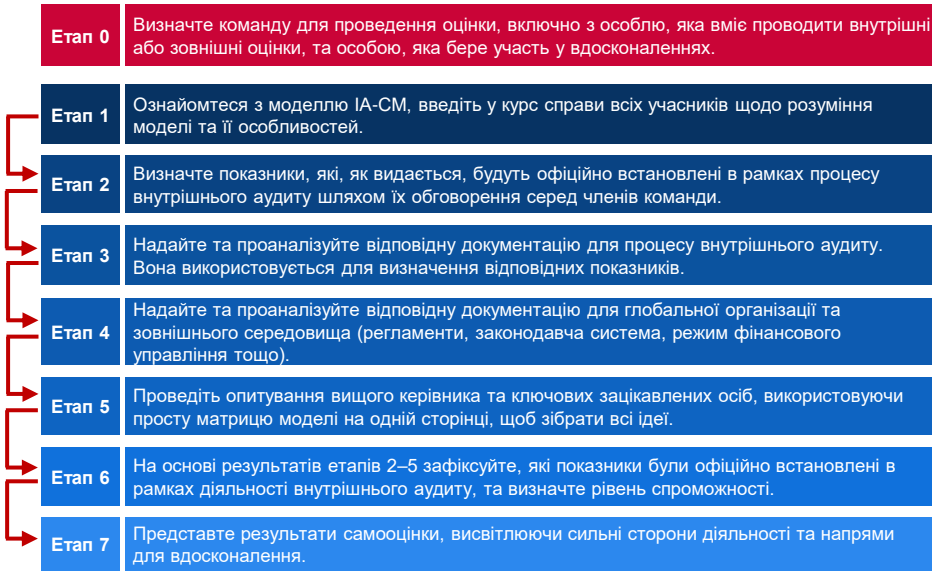
- Функції внутрішнього аудиту є невід'ємною частиною управління організацією та управління ризиками в ній.
- Внутрішній аудит — це добре керована бізнес-одиниця.
- Ризики вимірюються та управляються кількісно.
- Наявні необхідні навички та компетенції, що забезпечують спроможність оновлення та обміну знаннями (у рамках внутрішнього аудиту та всередині організації).

► **Рівень 5: оптимізація**
Навчання в організації та за межами для постійного вдосконалення
- Внутрішній аудит — це організація, яка постійно вчиться та вдосконалює процеси та вводить інновації.
- Внутрішній аудит використовує внутрішню інформацію організації та зовнішню інформацію для сприяння досягненню стратегічних цілей.
- Виконання передових/рекомендованих практик світового класу.
- Внутрішній аудит є критично важливою частиною структури управління організацією.
- Професійні та спеціалізовані навички найвищого рівня.
- Індивідуальні, на рівні підрозділу та організаційні показники ефективності повністю інтегровані для вдосконалення результативності діяльності.

Метод оцінки

Модель спроможності внутрішнього аудиту чітко розроблена для самооцінки. Вона містить детальні кроки для використання в моделі IA-CM та зразок пакету слайдів для налаштування. Перед початком самооцінки слід визначити конкретну команду, що включає як мінімум одну особу, яка вміє проводити внутрішні або зовнішні оцінки внутрішніх аудитів, та одну особу, яка бере участь у вдосконаленнях у цій сфері.

Рисунок 12. Етапи самооцінки за моделлю IC-AM



A.9 Глобальний індекс кібербезпеки (GCI)

Глобальний індекс кібербезпеки (GCI) — це ініціатива Міжнародного союзу електрозв'язку (МСЕ), спрямована на аналіз зобов'язань та ситуації в галузі кібербезпеки у всіх регіонах МСЕ: Африці, Америці, арабських державах, Азіатсько-тихоокеанському регіоні, СНД та Європі, та привертає увагу країн до важливих зобов'язань і рекомендованих практик. Мета GCI — допомогти країнам визначити напрями для вдосконалення в галузі кібербезпеки, а також мотивувати їх до дій щодо покращення свого рейтингу, тим самим сприяючи підвищенню загального рівня кібербезпеки у всьому світі.

Оскільки GCI є індексом, а не моделлю зрілості, він не використовує рівні зрілості, а скоріше бал для ранжування та порівняння загальних зобов'язань країн та регіонів щодо кібербезпеки.

Атрибути/виміри

Глобальний індекс кібербезпеки (GCI) базується на п'яти стовпах Глобальної програми кібербезпеки (GCA). Ці стовпи утворюють п'ять підіндексів GCI, а кожен включає набір показників. П'ять стовпів і показники такі:

i. **Правовий**: заходи, що базуються на існуванні правових інститутів і концепцій, що займаються кібербезпекою та кіберзлочинністю.
   - Законодавство про кіберзлочинність,
   - регулювання кібербезпеки і
   - Стримування/обмеження за законодавством про спам.

ii. **Технічний**: заходи, що базуються на існуванні технічних установ і концепцій, що займаються кібербезпекою.
   - Команди CERT/CIRT/CSRIT,
   - керівництво з впровадження стандартів,
   - орган зі стандартизації,
   - технічні механізми та спроможності, розгорнуті для вирішення проблем спаму,
   - використання хмарних технологій для цілей кібербезпеки і
   - механізми захисту дітей в Інтернеті.

iii. **Організаційний**: заходи, що базуються на існуванні інституцій координації політик та стратегій з розвитку кібербезпеки на національному рівні.
   - Національна стратегія кібербезпеки,
   - відповідальне агентство та
   - кібербезпека.

iv. **Розбудова спроможностей**: заходи, що базуються на існуванні науково-дослідних, освітніх і навчальних програм, сертифікованих фахівців та установ державного сектору, які сприяють розбудові спроможностей.
   - Кампанії з підвищення обізнаності громадськості,
   - керівництво із сертифікації та акредитації фахівців з кібербезпеки,
   - курси професійного навчання з кібербезпеки,
   - освітні програми або університетські навчальні програми з кібербезпеки,
   - програми НДДКР з кібербезпеки і
   - механізми стимулювання.

v. **Співпраця**: заходи, що базуються на існуванні партнерських відносин, концепцій співпраці та мереж обміну інформацією.
   - Двосторонні угоди,
   - багатосторонні угоди,
   - участь у міжнародних форумах/асоціаціях,
   - державно-приватне партнерство,
   - міжвідомче/внутрішньовідомче партнерство і
   - передові практики.

Метод оцінки

Індекс GCI — це інструмент самооцінки, побудований за допомогою проведення опитування[30] у форматі альтернативних запитань та запитань з варіантами відповідей і без варіантів. Використання альтернативних відповідей виключає оцінювання, засноване на інтерпретації, та будь-яку можливу упередженість щодо певних типів відповідей. Запитання з варіантами відповідей економлять час і дозволяють більш точно аналізувати дані. До того ж проста дихотомічна шкала дозволяє проводити швидше і складніше оцінювання, оскільки не вимагає тривалих відповідей, що прискорює та впорядковує процес надання відповідей та подальшого їх оцінювання. Респондент повинен лише підтвердити наявність або відсутність певних попередньо визначених рішень з питань кібербезпеки. Механізм інтернет-опитування, який використовується для збору відповідей та завантаження відповідних матеріалів, дозволяє групі експертів отримати корисний досвід та набір тематичних якісних оцінок.

[30] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCIv4_English.pdf

Загальний процес відповідно до індексу GCI реалізується таким чином.

- Усім учасникам надсилається лист із запрошенням, в якому надається інформація про проєкт та висловлюється прохання визначити контактну особу, яка відповідає за збір усіх відповідних даних та заповнення онлайн-анкети GCI. Під час онлайн-опитування MCE офіційно запрошує затверджену контактну особу для надання відповідей в анкеті.
- Первинний збір даних (для країн, які не відповідають на анкету):
  - MCE розробляє початковий проєкт відповіді на анкету, використовуючи загальнодоступні дані та онлайн-дослідження;
  - проєкт анкети надсилається контактній особі для ознайомлення;
  - контактні особи покращують її точність, а потім повертають проєкт анкети;
  - виправлений проєкт анкети надсилається кожній контактній особі для остаточного затвердження; і
  - затверджена анкета використовується для аналізу, виставлення балів і побудови рейтингу.
- Вторинний збір даних (для країн, які відповідають на анкету):
  - MCE визначає будь-які відсутні відповіді, супровідні документи, посилання тощо;
  - контактна особа покращує точність відповідей, де це необхідно;
  - виправлений проєкт анкети надсилається кожній контактній особі для остаточного затвердження; і
  - затверджена анкета використовується для аналізу, виставлення балів і побудови рейтингу.

A.10 Індекс кіберпотужності (CPI)

Індекс кіберпотужності (CPI) був створений в рамках дослідної програми компанії "Економіст Інтеліджене Юніт", спонсорованої Бузом Алленом Гамільтоном у 2011 році. Індекс CPI є "динамічною кількісною та якісною моделлю [...], яка вимірює конкретні атрибути кіберсередовища за чотирма рушійними факторами кіберпотужності: нормативно-правове регулювання; економічний і соціальний контекст; технологічна інфраструктура; та галузевий застосунок, який досліджує цифровий прогрес у ключових галузях"[31]. Ціллю індексу кіберпотужності є оцінка ефективності спроможності країн G20 протистояти кібератакам та розгортати необхідну цифрову інфраструктуру для успішної та безпечної економіки. Оцінка ефективності, отримана на основі CPI, зосереджена на 19 країнах з G20 (крім ЄС). Потім індекс надає рейтинг країн за кожним показником.

Атрибути/виміри

Індекс кіберпотужності (CPI) базується на чотирьох рушійних факторах кіберпотужності. Потім кожну категорію вимірюють за допомогою кількох показників, аби виставити кожній країні певний бал. Категорії та стовпи такі:

i. **Нормативно-правове регулювання**
   - Зобов'язання державних органів щодо розвитку кіберсфери
   - Політики кіберзахисту
   - Кіберцензура (або її відсутність)
   - Ефективність політичних дій
   - Захист інтелектуальної власності

ii. **Економічний та соціальний контекст**
   - Освітні рівні
   - Технічні навички
   - Відкритий характер торгівлі
   - Рівень інновацій у бізнес-середовищі

iii. **Технологічна інфраструктура**
   - Доступ до інформаційно-комунікаційних технологій
   - Якість інформаційно-комунікаційних технологій
   - Доступність інформаційно-комунікаційних технологій
   - Витрати на інформаційні технології
   - Кількість захищених серверів

[31] www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf

iv. Галузевий застосунок

- Інтелектуальні енергосистеми
- Електронна система охорони здоров'я E-Health
- Електронна комерція
- Інтелектуальне транспортування
- Електронний уряд

Метод оцінки

Індекс CPI — це кількісна та якісна модель нарахування балів. Оцінка була проведена компанією "Економіст Інтеліджанс Юніт" з використанням кількісних показників із наявних статистичних джерел та шляхом надання прогнозних показників, коли бракувало даних. Основними використаними джерелами є дані від компанії "Економіст Інтеліджанс Юніт", Організації ООН з питань освіти, науки та культури (ЮНЕСКО), Міжнародного союзу електрозв'язку (МСЕ) та Світового банку.

A.11 Індекс кіберпотужності (CPI)

У цьому розділі узагальнено основні результати аналізу наявних моделей зрілості. Таблиця 5. Огляд проаналізованих **моделей** зрілості надає огляд основних характеристик кожної моделі відповідно до модифікованої моделі Беккера. Таблиця 6. Порівняння рівнів зрілості. Характеристики високого рівня зрілості аналізованих моделей. У таблиці 7 наведено огляд вимірів або атрибутів, що використовуються в кожній моделі.

Таблиця 5. Огляд проаналізованих моделей зрілості

Назва моделі	Первинна установа	Мета	Ціль	Кількість рівнів	Кількість атрибутів	Метод оцінки	Представлення результатів
Модель зрілості спроможностей кібербезпеки для держав (CMM)	Глобальний центр спроможностей кібербезпеки Оксфордського університету	Збільшити масштаби та ефективність розвитку спроможностей кібербезпеки на міжнародному рівні	Країни	5	5 основних вимірів	Співпраця з місцевою організацією з метою доопрацювання моделі перед її застосуванням у національному контексті	5-секційний радар
Модель зрілості спроможностей кібербезпеки (C2M2)	Департамент енергетики США (DOE)	Допомога організаціям оцінити та вдосконалити свої програми з кібербезпеки та зміцнити свою експлуатаційну стійкість.	Організації з всіх секторів, всіх типів і розмірів	4	10 основних сфер	Методологія та набір інструментів для самооцінювання	Картка балів з круговими діаграмами
Керівництво для удосконалення кібербезпеки критично важливої інфраструктури	Національний інститут стандартів і технології (NIST)	Керівництво спрямоване на управління діяльністю в галузі кібербезпеки та управління ризиками в організаціях	Організації	Немає даних (4 яруси)	5 основних функцій	Самооцінка	–
Катарська модель зрілості спроможностей кібербезпеки (Q-C2M2)	Факультет права Катарського університету	Забезпечення дієвої моделі, яка може бути використана для оцінки ефективності, вимірювання та розвитку Керівництва з кібербезпеки Катару	Катарські організації	5	5 основних сфер	–	–
Сертифікація моделі зрілості кібербезпеки (CMMC)	Міністерством оборони США (DoD)	Заохочувати передові практики кібербезпеки для захисту інформації	Організації сектору оборонної промислової бази (DIB).	5	17 основних сфер	Оцінка сторонніми аудиторами	–
Модель зрілості кібербезпеки громади (CCSMM)	Центр безпеки та ефективності інфраструктури Техаського університету.	Визначити поточний статус громади стосовно її кіберготовності та надати дорожню карту для громад, якої слід дотримуватися у своїх зусиллях з підготовки	Громади (органи місцевого самоврядування або органи штату)	5	6 основних вимірів	Оцінка в громадах на основі даних, отриманих від державних і федеральних правоохоронних органів	–
Модель зрілості інформаційної безпеки для Керівництва NIST з кібербезпеки (ISMM)	Коледж комп'ютерних наук та техніки Університету нафти та корисних копалин короля Фахда, Дахран, Саудівська Аравія.	Надання організаціям можливості вимірювати свій прогрес у впровадженні з часом, аби гарантувати, що вони зберігають бажаний стан безпеки	Організації	5	23 оцінені сфери	–	–
Модель спроможності внутрішнього аудиту (IA-CM) для державного сектору	Інститут внутрішніх аудиторів Фонду досліджень	Розбудова спроможності внутрішнього аудиту та адвокація шляхом самооцінки в державному секторі.	Організації державного сектору	5	6 елементів	Самооцінка	–
Глобальний індекс кібербезпеки (GCI)	Міжнародний союз електрозв'язку (MCE)	Переглянути зобов'язання та ситуацію у сфері кібербезпеки і допомогти країнам визначити напрями для вдосконалення у сфері кібербезпеки	Країни	НЕМАЄ ДАНИХ	5 стовпів	Самооцінка	Рейтингова таблиця
Індекс кіберпотужності (CPI)	Компанія "Економіст Інтеліджанс Юніт" та Буз Аллен Гамільтон	Оцінка ефективності спроможності країн G20 протистояти кібератакам та розгортати необхідну цифрову інфраструктуру для успішної та безпечної економіки.	Країни G20	НЕМАЄ ДАНИХ	4 категорії	Оцінка ефективності, проведена компанією "Економіст Інтеліджанс Юніт"	Рейтингова таблиця

Таблиця 6. Порівняння рівнів зрілості

Модель	Рівень 1	Рівень 2	Рівень 3	Рівень 4	Рівень 5
Модель зрілості спроможностей кібербезпеки для держав (CMM)	**Запуск** Або не існує зрілості кібербезпеки, або вона має дуже ембріональний характер. Можливо, були початкові дискусії щодо розбудови спроможностей кібербезпеки, але конкретних дій не було вчинено. На цьому етапі відсутні помітні докази.	**Творення** Почали зростати та формуватися деякі особливості аспектів, але можуть бути ситуативними, дезорганізованими, погано визначеними або просто "новими". Однак докази цієї діяльності можна наочно продемонструвати.	**Встановлення** Запроваджені та працюють елементи аспекту. Однак немає добре продуманого розгляду відповідного розподілу ресурсів. Було прийнято мало компромісних рішень щодо "відповідних" інвестицій у різні елементи аспекту. Однак аспект функціональний і визначений.	**Стратегічний** Було зроблено вибір щодо того, які частини аспекту є важливими, а які менш важливими для конкретної організації чи країни. Стратегічний етап відображає той факт, що цей вибір був зроблений залежно від обставин країни або організації.	**Динамічний** Запроваджені чіткі механізми зміни стратегії залежно від переважних обставин, таких як технологія середовища загрози, глобальний конфлікт або суттєві зміни в одній зі сфер, яка розглядається (наприклад, кіберзлочинність або конфіденційність/приватність). Динамічні організації розробили методи поступової зміни стратегій. Швидке прийняття рішень, перерозподіл ресурсів та постійна увага до мінливого середовища є особливістю цього етапу.
Модель зрілості спроможностей кібербезпеки (C2M2)	**MIL0** Практики не виконуються.	**MIL1** Початкові практики виконуються, але можуть бути ситуативними.	**MIL2** Характеристики управління: практика документується; для забезпечення процесу надаються належні ресурси; персонал, який реалізує практику, має адекватні навички та знання; і передані відповідальність та повноваження для виконання практик. Характеристика підходу: практика є повнішою або більш вдосконаленою, ніж на MIL1.	**MIL3** Характеристики управління: у діяльності керуються політикою (або іншими організаційними директивами); цілі ефективності діяльності у сфері визначаються та контролюються для відстеження досягнень; і задокументована практика для діяльності у сфері стандартизована та вдосконалена на всьому підприємстві. Характеристика підходу: практика є повнішою або більш вдосконаленою, ніж на MIL2.	–
Модель зрілості інформаційної безпеки для Керівництва НІСТ з кібербезпеки (ISMM)	**Процес виконання**	**Процес керування**	**Процес встановлення**	**Процес передбачення**	**Процес оптимізації**
Катарська модель зрілості спроможностей кібербезпеки (Q-C2M2)	**Ініціювання** Використовує спеціальні практики та процес з кібербезпеки в межах деяких сфер.	**Розробка** Впроваджені політики та практика для розвитку і вдосконалення діяльності з кібербезпеки в межах сфер з метою запропонувати нові заходи для реалізації.	**Впровадження** Ухвалені політики щодо впровадження всіх заходів з кібербезпеки в межах сфер з метою завершення реалізації в певний час.	**Адаптація** Інспектує і переглядає діяльність з кібербезпеки та адаптує практику на основі прогнозних показників, отриманих із попереднього досвіду та заходів.	**Гнучкість** Продовжує практикувати адаптаційний етап із додатковим акцентом на гнучкість і швидкість під час реалізації діяльності у сферах.

Модель	Рівень 1	Рівень 2	Рівень 3	Рівень 4	Рівень 5
Сертифікація моделі зрілості кібербезпеки (CMMC)	**Процеси: виконання** Оскільки організація може лише виконувати ці практики нерегулярно і може покладатися або не покладатися на документацію, процес зрілості не оцінюється на рівні 1. **Практики: базова кібергігієна** Рівень 1 фокусується на захисті інформації FCI (Інформація федерального уряду) і складається лише з практик, які відповідають основним вимогам захисту.	**Процеси: задокументовані** Рівень 2 вимагає, аби організація встановила та задокументувала практики та політики для управління процесом впровадження своїх зусиль у рамках стандарту CMMC. Документація практик дозволяє людям виконувати їх у повторюваній формі. Організації розвивають зрілі спроможності, документуючи свої процеси, а потім практикуючи їх, як задокументовано. **Практики: кібергігієна середнього рівня** Рівень 2 слугує етапом просування від рівня 1 до рівня 3 і складається з підгрупи вимог безпеки, зазначених у NIST SP 800-171, а також практик з інших стандартів і джерел.	**Процеси: керований** Рівень 3 вимагає, аби організація створила, підтримувала та надавала ресурси для плану, що демонструє управління діяльністю щодо впровадження практики. План може включати інформацію про завдання, цілі, плани заходів, ресурси, необхідну підготовку та залучення відповідних зацікавлених осіб. **Практики: хороша кібергігієна** Рівень 3 зосереджується на захисті контрольованої відкритої інформації та охоплює всі вимоги до безпеки, зазначені в NIST SP 800-171, а також додаткові практики з інших стандартів та джерел з метою пом'якшення загроз.	**Процеси: переглянутий** Рівень 4 вимагає, аби організація перевіряла та вимірювала практики щодо ефективності. На додаток до вимірювання практик щодо ефективності організації на цьому рівні можуть вживати коригувальних заходів, коли це необхідно, та регулярно інформувати вище керівництво про стан або проблемні питання. **Практики: дуже активний** Рівень 4 зосереджений на захисті контрольованої відкритої інформації та охоплює підгрупу посилених вимог безпеки. Ці практики покращують спроможності організації виявляти та реагувати щодо спрямування уваги та адаптації до змін тактики, технік та процедур.	**Процеси: оптимізація** Рівень 5 вимагає від організації проведення стандартизації та оптимізації впровадження процесів в рамках організації. **Практики: розвинений/дуже активний** Рівень 5 зосереджений на захисті контрольованої відкритої інформації. Додаткові практики збільшують глибину та складність спроможностей кібербезпеки.
Модель зрілості кібербезпеки громади (CCSMM)	**Обізнаний про безпеку** Основною темою діяльності на цьому рівні є інформування приватних осіб та організацій про загрози, проблеми та проблемні питання, пов'язані з кібербезпекою.	**Розвиток процесу** Рівень призначений допомогти громадам встановити та вдосконалити процеси безпеки, необхідні для ефективного розв'язання питань кібербезпеки.	**Доступна інформація** Розроблений для вдосконалення механізмів обміну інформацією в межах громади, аби громада могла ефективно співвідносити, на перший погляд, розрізнену інформацію.	**Розвиток тактики** Елементи цього рівня спроєктовані для розробки кращих та більш активних методів виявлення та реагування на атаки. До цього рівня більшість превентивних методів повинні вже бути впроваджені.	**Повна операційна спроможність безпеки** Цей рівень представляє ті елементи, які мають бути запроваджені для будь-якої організації, аби вважатися повністю оперативно готовою до вирішення будь-якого типу кіберзагрози.
Модель спроможності внутрішнього аудиту (IA-CM) для державного сектору	**Початковий** Немає стійких, повторюваних спроможностей — залежить від індивідуальних зусиль	**Інфраструктура** Стійкі та повторювані практики та процедури	**Інтегрований** Управлінська та професійна практика застосовуються рівномірно	**Керований** Інтегрує інформацію з усієї організації для вдосконалення управління нею та управління ризиками	**Оптимізація** Навчання в організації та за межами для постійного вдосконалення

Таблиця 7. Порівняння атрибутів/вимірів

	Модель зрілості спроможностей кібербезпеки для держав (CMM)	Модель зрілості спроможностей кібербезпеки (C2M2)	Катарська модель зрілості спроможностей кібербезпеки (Q-C2M2)	Сертифікація моделі зрілості кібербезпеки (CMMC)	Сертифікація моделі зрілості кібербезпеки (CMMC)	Модель зрілості інформаційної безпеки для Керівництва НІСТ з кібербезпеки (ISMM)	Керівництво для удосконалення кібербезпеки критично важливої інфраструктури	Глобальний індекс кібербезпеки (GCI)	Індекс кіберпотужності (CPI)
Рівні	П'ять вимірів, розділених на кілька факторів, що, зі свого боку, включають численні аспекти та показники (рисунок 4)	Десять сфер, у тому числі унікальна ціль управління та декілька цілей підходу (рисунок 6)	П'ять сфер розділені на підсфери	Сімнадцять сфер детально описані в процесах і від однієї до багатьох спроможностей, які потім детально описані в практиках (рисунок 9)	Шість основних вимірів	Двадцять три оцінені сфери	П'ять функцій з основними ключовими категоріями та підкатегоріями (рисунок)	П'ять стовпів, у тому числі кілька показників	Чотири категорії з кількома показниками
Атрибути /виміри	i. Винайдення політики та стратегії кібербезпеки ii. Заохочення відповідальної культури кібербезпеки в суспільстві iii. Розвиток знань з кібербезпеки iv. Створення ефективного нормативно-правового регулювання v. Контроль ризиків за допомогою стандартів, організацій та технологій	i. Управління ризиками ii. Управління активами, змінами та конфігурацією iii. Управління ідентифікацією та доступом iv. Управління загрозами та вразливістю v. Ситуативна обізнаність vi. Реагування на події та інциденти vii. Управління ланцюгами постачання та зовнішніми взаємозалежностями viii. Управління персоналом ix. Архітектура кібербезпеки x. Управління програмою кібербезпеки	i. Зрозуміти (кіберуправління, активи, ризики та навчання) ii. Гарантувати (захист даних, безпеку технологій, безпеку контролю доступу, безпеку комунікацій та безпеку персоналу) iii. Викривати (моніторинг, управління інцидентами, виявлення, аналіз і викриття) iv. Реагувати (планування реагування, пом'якшення наслідків та комунікація під час реагування) v. Підтримувати (планування відновлення, управління цілісністю процесу, вдосконалення та зовнішні взаємозалежності).	i. Контроль доступу ii. Управління активами iii. Аудит та підзвітність iv. Обізнаність та навчання v. Управління конфігураціями vi. Ідентифікація та автентифікація vii. Реагування на інциденти viii. Підтримка реалізації ix. Медіазахист x. Безпека персоналу xi. Фізичний захист xii. Відновлення роботи xiii. Управління ризиками xiv. Оцінка безпеки xv. Ситуативна обізнаність xvi. Захист системи та комунікацій xvii. Цілісність системи та інформації	i. Загрози вирішуються ii. Метрики iii. Обмін інформацією iv. Технологія v. Навчання vi. Тестування	i. Управління активами ii. Бізнес-середовище iii. Управління iv. Оцінка ризику v. Стратегія управління ризиками vi. Оцінка відповідності vii. Контроль доступу viii. Обізнаність та навчання ix. Безпека даних x. Процеси та процедури захисту інформації xi. Підтримка реалізації xii. Технологія захисту xiii. Аномалії та події xiv. Безперервний моніторинг безпеки xv. Процеси виявлення xvi. Планування реагування xvii. Комунікація реагування xviii. Аналіз реагування xix. Пом'якшення наслідків реагування xx. Вдосконалення реагування xxi. Планування відновлення xxii. Вдосконалення відновлення xxiii. Комунікація відновлення	i. Визначити ii. Захистити iii. Виявити iv. Реагувати v. Відновлювати	i. Правовий ii. Технічний iii. Організаційний iv. Розвиток спроможностей v. Співпраця	i. Нормативно-правове регулювання ii. Економічний та соціальний контекст iii. Технологічна інфраструктура iv. Галузевий застосунок

ДОДАТОК B — СПИСОК ДЖЕРЕЛ КАБІНЕТНОГО ДОСЛІДЖЕННЯ

Almuhammadi, S. and Alsaleh, M. (2017) 'Information Security Maturity Model for Nist Cyber Security Framework', in Computer Science & Information Technology (CS & IT). Sixth International Conference on Information Technology Convergence and Services, Academy & Industry Research Collaboration Center (AIRCC).

Almuhammadi, S. and Alsaleh, M. (2017) 'Information Security Maturity Model for Nist Cyber Security Framework', in Computer Science & Information Technology (CS & IT). Доступне за посиланням: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. et al. (2016) Stocktaking, analysis and recommendations on the protection of CIIs. Доступне за посиланням: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. et al. (2009) Developing Maturity Models for IT Management – A Procedure Model and its Application. Доступне за посиланням: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Belgian Government (2012) Cyber Security Strategy. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. et al. (2018) Developing Cybersecurity Capacity: A proof-of-concept implementation guide. Американський аналітичний центр RAND Corporation. Доступне за посиланням: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR207 2.pdf

Bourgue, R. (2012) 'Introduction to Return on Security Investment'. Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019) "Cybersecurity Capability Maturity Model (C2M2) Version 2.0. Доступне за посиланням https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Center for Security Studies (CSS), ETH Zürich (2019) National Cybersecurity Strategies in Comparison – Challenges for Switzerland. Доступне за посиланням: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Council of Ministers (2019) Portuguese Official Journal, Series 1 — No. 108 – Resolution of the Council of Ministers No. 92/2019. Доступне за посиланням: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016) Cybersecurity Capacity Maturity Model for Nations (CMM). Оксфордський університет. Зрілість команди CSIRT — інструмент самооцінки (без дати). Доступне за посиланням: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

CyberCrime@IPA project of the Council of Europe and the European Union, Global Project on Cybercrime of the Council of Europe and European Union Cybercrime Task Force (2011)

Спеціалізовані підрозділи з питань кіберзлочинності — вивчення корисного досвіду. Доступне за посиланням: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Система звітування та аналізу інцидентів кібербезпеки — інструмент візуального аналізу (без дати). Доступне за посиланням: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017) Public Private Partnerships (PPP).

Darra, E. (no date) 'Welcome to the NCSS Training Tool'.

Dekker, M. A. C. (2014) Technical Guideline on Incident Reporting. Доступне за посиланням: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014) Technical Guideline on Security Measures. Доступне за посиланням: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015) Guideline on Threats and Assets. Доступне за посиланням: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Цифрова Словенія (2016). Стратегія кібербезпеки. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *et al.* (2014) *Privacy and data protection by design – from policy to engineering.* Доступне за посиланням: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Європейська комісія (2012). Регламент Європейського Парламенту та Ради про електронну ідентифікацію та довірчі послуги для електронних трансакцій у межах внутрішнього ринку. Доступне за посиланням: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0238&from=EN

Європейське агентство з питань мережевої та інформаційної безпеки (2012). Національна стратегія кібербезпеки: практичний посібник з розробки та виконання. Іракліон: ENISA.

Європейське агентство з питань мережевої та інформаційної безпеки (2012). Національна стратегія кібербезпеки: встановлення курсу національних зусиль щодо зміцнення безпеки в кіберпросторі. Іракліон: ENISA.

Європейське агентство з питань мережевої та інформаційної безпеки (2016). Настанови для МСП щодо безпеки обробки персональних даних.

Європейське агентство з питань мережевої та інформаційної безпеки (2016). Посібник рекомендованих стандартів щодо Національної стратегії кібербезпеки: розробка та впровадження національних стратегій кібербезпеки. Іракліон: ENISA.

Європейський Союз та Європейське агентство з питань мережевої та інформаційної безпеки (2017). Довідник з безпеки обробки персональних даних. Доступне за посиланням: http://dx.publications.europa.eu/10.2824/569768

European Union and Agency for Network and Information Security (2014) *ENISA CERT inventory inventory of CERT teams and activities in Europe*. Доступне за посиланням: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Адміністрація Президента (2015). Меморандум керівників виконавчих органів і відомств. Доступне за посиланням: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Федеральна канцелярія Республіки Австрія (2013). Австрійська стратегія кібербезпеки. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Федеральне міністерство внутрішніх справ (2011). Стратегія кібербезпеки для Німеччини. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Ferette, L. (2016) NIS Directive and national (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Доступне за посиланням: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., European Union and European Network and Information Security Agency (2015) The 2015 report on national and international cyber security exercises: survey, analysis and recommendations. Доступне за посиланням: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Офіс прем'єр-міністра Франції (2014). Французька національна стратегія цифрової безпеки. Доступне за посиланням: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Galan Manso, C. et al. (2015) Information security and privacy standards for SMEs: recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Доступне за посиланням: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ghent University et al. (2017) 'Evaluating Business Process Maturity Models', Journal of the Association for Information Systems. Доступне за посиланням: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Уряд Болгарії (2015). Національна стратегія кібербезпеки. Кіберстійка Болгарія, 2020.

Уряд Хорватії (2015). Національна стратегія кібербезпеки Республіки Хорватія. Доступне за посиланням: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Уряд Греції (2017). Національна стратегія кібербезпеки. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Уряд Угорщини (2018). Стратегія безпеки мережевих та інформаційних систем. Доступне за посиланням: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Уряд Ірландії (2019). Національна стратегія кібербезпеки. Доступне за посиланням: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Уряд Іспанії (2019). Національна стратегія кібербезпеки. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Інститут внутрішніх аудиторів (вид.) (2009). Модель спроможності внутрішнього аудиту (IA-CM) для державного сектору: огляд та посібник із застосування. Алтамонте-Спрінгс, Флорида: Інститут внутрішніх аудиторів, Фонд досліджень.

Міжнародний союз електрозв'язку (MCE) (2018). Глобальний індекс кібербезпеки. Доступне за посиланням: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Міжнародний союз електрозв'язку (MCE) (2018). Посібник з розробки національної стратегії кібербезпеки. Доступне за посиланням: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B. (2019) 'Towards a Qatar Cybersecurity Capability Maturity Model with a Legislative Framework', International Review of Law.

Уряд Латвії (2014). Стратегія кібербезпеки Латвії. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. et al. (2014) An evaluation framework for national cyber security strategies. Іракліон: ENISA. Доступне за посиланням: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. *et al.* (2014) *Methodologies for the identification of critical information infrastructure assets and services: guidelines for charting electronic data communication networks.* Доступне за посиланням: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Міністерство з питань конкуренції та цифрової економіки, морських справ та економіки сфери послуг (2016). Мальтійська стратегія кібербезпеки. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Міністерство економічних справ та комунікацій (2019). Стратегія кібербезпеки — Республіка Естонія. Доступне за посиланням: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Міністерство національної оборони Республіки Литва (2018). Національна стратегія кібербезпеки.

Національний центр кібербезпеки (2015). Національна стратегія кібербезпеки Республіки Чехія. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Національні стратегії кібербезпеки — інтерактивна мапа (без дати). Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Інструмент оцінки національної стратегії кібербезпеки (2018). Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Національний інститут стандартів і технології (2018), Керівництво для удосконалення кібербезпеки критично важливої інфраструктури, версія 1.1. Gaithersburg, MD: National Institute of Standards and Technology (Національний інститут стандартів і технології). Доступне за посиланням: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Object Management Group (2008) Business Process Maturity Model. Доступне за посиланням: https://www.omg.org/spec/BPMM/1.0/PDF

ОЕСР, Європейський Союз та Спільний науково-дослідний центр — Європейська комісія (2008). Довідник з побудови комплексних показників: методологія та посібник користувача. ОЕСР. Доступне за посиланням: https://www.oecd.org/sdd/42495745.pdf.

Офіс уповноваженого з питань електронного зв'язку та поштового регулювання (2012). Стратегія кібербезпеки Республіки Кіпр.

Офіційний вісник Європейського Союзу (2008) ДИРЕКТИВА РАДИ 2008/114/ЄС від 8 грудня 2008 року про ідентифікацію та призначення європейських критичних інфраструктур та оцінку необхідності вдосконалення їх захисту. Доступне за посиланням:: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Організація економічного співробітництва та розвитку (ОЕСР) (2012). Формування та реалізація політики кібербезпеки на переломному етапі. Доступне за посиланням: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012) 'National Cyber Security Strategies – Practical Guide on Development and Execution'.

Ouzounis, E. (2012) Good Practice Guide on National Exercises.

Portesi, S. (2017) Improving Cooperation between CSIRTs and Law Enforcement: Legal and Organisational Aspects.

Голова Ради Міністрів Італії (2017). Італійський план дій з кібербезпеки. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Рада міністрів (2019). Офіційний вісник Республіки Польща. Доступне за посиланням: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Румунський уряд (2013). Стратегія кібербезпеки Румунії. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. and European Union Agency for Cybersecurity (2019) Good practices in innovation on cybersecurity under the NCSS: good practices in innovation on cybersecurity under the national cyber security strategies. Доступне за посиланням: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Секретаріат Комітету з питань безпеки (2019). Стратегія кібербезпеки Фінляндії 2019 року. Доступне за посиланням: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Уряд Словаччини (2015). Концепція кібербезпеки Республіки Словаччина. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R. (2015) Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010

Smith, R. (2016) 'Directive 2010/41/EU of the European Parliament and of the Council of 7 July 2010', in Smith, R., Core EU Legislation. London: Macmillan Education. Доступне за посиланням: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Stavropoulos, V. (2017) European Cyber Security Month 2017.

Уряд Швеції (2017) Nationell strategi för samhällets informations- och cybersäkerhet. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Уряд Данії — Міністерство фінансів (2018). Данська стратегія кібер- та інформаційної безпеки. Доступне за посиланням: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Федеральна рада (2018). Національна стратегія захисту Швейцарії від кіберризиків.

Урядова рада Люксембургу (2018) Національна стратегія кібербезпеки. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Уряд Нідерландів (2018). Національний план дій з кібербезпеки. Доступне за посиланням: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

Білий дім (2018). Стратегія кібербезпеки Сполучених Штатів Америки. Доступне за посиланням: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P., et al. (2011) Cyber Europe Report. Доступне за посиланням: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. and European Network and Information Security Agency (2013) *National-level risk assessments: an analysis report.* Доступне за посиланням: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., et al. (2015) Report on cyber-crisis cooperation and management. Доступне за посиланням: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A., et al. (2015) Report on cyber crisis cooperation and management: common practices of EU-level crisis management and applicability to cyber crises. Доступне за посиланням: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

Національна стратегія кібербезпеки Великої Британії 2016—2021 рр. (2016). Доступне за посиланням: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Університет Інсбрука та інші (2009). Розуміння моделей зрілості.

Wamala, D. F. (2011) 'ITU National Cybersecurity Strategy Guide. Доступне за посиланням: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007) 'The Community Cyber Security Maturity Model', in 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07).

ДОДАТОК C — ІНШІ ДОСЛІДЖЕНІ ЦІЛІ

Детально описані нижче цілі були досліджені в рамках фази кабінетного дослідження та співбесід, проведених ENISA. Зазначені нижче цілі не є частиною Керівництва з оцінки національних спроможностей, але вони висвітлюють теми, які варто обговорити. Кожен із поданих нижче підрозділів дасть пояснення, чому ціль була відкинута.

- Розробити галузеві стратегії кібербезпеки
- Боротися з кампаніями дезінформації
- Забезпечити використання передових технологій (5G, ШІ, обчислення за допомогою квантових комп'ютерів тощо)
- Забезпечити суверенітет даних
- Забезпечити стимули для розвитку галузі кіберстрахування

Розробити галузеві стратегії кібербезпеки

Прийняття галузевих стратегій, спрямованих на секторні втручання та стимули, безумовно, забезпечує посилення децентралізованих спроможностей. Це особливо підходить для країн-членів, чиї ООП повинні мати справу з різними керівництвами та регламентами і де існує багато взаємозалежностей через трансверсальний характер кібербезпеки. Дійсно, у кількох країнах-членах можна нарахувати десятки національних органів влади та регуляторних органів, які володіють інформацією щодо особливостей кожного сектору та мають мандат забезпечувати виконання конкретного регламенту для кожного сектору.

Наприклад, Данія запустила шість цільових стратегій, спрямованих на дії та заходи щодо кібербезпеки та інформаційної безпеки в найбільш критично важливих секторах для розвитку більш потужних децентралізованих спроможностей у сфері кібербезпеки та інформаційної безпеки. Кожен "галузевий підрозділ" буде сприяти оцінці загроз на галузевому рівні та, серед іншого, моніторингу, підготовці, встановленню систем безпеки, обміну знаннями та інструкціям. Галузеві стратегії охоплюють такі сектори:

- енергетику,
- охорону здоров'я,
- транспорт,
- телекомунікації,
- фінанси та
- морську сферу.

Інші країни-члени висловили зацікавленість у розгляді галузевих стратегій кібербезпеки, які б містили всі нормативні вимоги. Однак слід зазначити, що така ціль може не підходити для всіх країн-членів залежно від їх розміру, національної політики та зрілості. Значні труднощі в забезпеченні того, аби Керівництво могло враховувати всі особливості, призвели до того, що ENISA не включало цю ціль в Керівництво.

Боротися з кампаніями дезінформації

Країни-члени інтегрують захист основних принципів, таких як права людини, прозорість та довіра громадськості, до своїх національних стратегій кібербезпеки. Це дуже важливо, особливо якщо йдеться про дезінформацію, яка поширюється за допомогою традиційних засобів масової інформації або платформ соціальних мереж. Крім того, кібербезпека в цей час є однією з найбільших виборчих викликів. Дійсно, такі дії, як поширення неправдивої інформації або негативна пропаганда, спостерігалися в різних країнах напередодні важливих виборів.

Ця загроза може підірвати демократичний процес ЄС. На європейському рівні Комісія окреслила План дій[32] для активізації зусиль з протидії дезінформації в Європі: цей план зосереджений на 4 ключових сферах (виявлення, співпраця, взаємодія з онлайн-платформами та обізнаність) і слугує для розбудови спроможностей ЄС та зміцнення співпраця між країнами-членами.

4 з 19 опитаних країн висловили намір розв'язати проблему дезінформації та пропаганди у своїх національних стратегіях кібербезпеки.

Наприклад, Національна стратегія кібербезпеки Франції[33] зазначає, що "відповідальність держави полягає в тому, аби інформувати громадян про ризики технологій маніпуляції та пропаганди, які використовуються зловмисниками в Інтернеті. Наприклад, після терактів проти Франції у січні 2015 року уряд створив інформаційну платформу про ризики, пов'язані з ісламською радикалізацією через електронні мережі комунікації: "Stop-djihadisme.gouv.fr". Цей підхід міг бути поширеним для реагування на інші явища пропаганди або дестабілізації.

В іншому прикладі, у Національній стратегії кібербезпеки Польщі[34] на 2019—2024 рр. зазначається, що "проти маніпулятивної діяльності, наприклад, кампаній поширення дезінформації, необхідні системні дії для розвитку обізнаності громадян у контексті перевірки правдивості інформації та реагування на спроби її спотворення".

Однак під час співбесід, проведених ENISA, кілька країн-членів поділились інформацією, що вони не розглядають цю проблему як частину своєї Національної стратегії кібербезпеки як загрозу кібербезпеці, а розв'язують цю проблему на ширшому суспільному рівні, наприклад, за допомогою політичних ініціатив.

Забезпечити використання передових технологій (5G, ШІ, обчислення за допомогою квантових комп'ютерів тощо)

Оскільки поточне середовище кіберзагроз продовжує розширюватися, розвиток нових технологій, швидше за все, призведе до збільшення інтенсивності та кількості кібератак та диверсифікації методів, засобів і цілей, що застосовуються суб'єктами загроз. Тим часом ці нові технологічні рішення у формі найсучасніших технологій потенційно можуть стати структурними елементами європейського цифрового ринку. З метою захисту щораз більшої цифрової залежності країн-членів та у зв'язку з появою нових технологій слід встановити стимули та повноцінну політику для підтримки безпечного та надійного розвитку та впровадження цих технологій в ЄС.

На етапі кабінетного дослідження, проведеного на основі національних стратегій кібербезпеки країн-членів, були виокремлені такі передові технології, що представляють інтерес для країн-членів: 5G, ШІ, квантове обчислення, криптографія, граничні обчислення, підключені до мережі та автономні транспортні засоби, супермасиви даних та "розумні дані", блокчейн, робототехніка та інтернет речей.

Більш конкретно, на початку 2020 року Європейська комісія опублікувала повідомлення, в якому закликає країни-члени вжити заходів для реалізації комплексу заходів, рекомендованих у висновках до інструментарію для 5G[35]. Цей інструментарій для 5G з'явився після Рекомендації (ЄС) 2019/534 щодо кібербезпеки мереж 5G, прийнятої Комісією у 2019 році, яка закликає до впровадження єдиного європейського підходу до безпеки мереж 5G[36].

Під час співбесід, проведених ENISA, було підкреслено, що ця тема є скоріше трансверсальною темою, яка розглядається в рамках усієї Національної стратегії кібербезпеки, а не як конкретна ціль *як така*.

[32] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[33] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[34] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
[35] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission
[36] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019H0534

Забезпечити суверенітет даних

З одного боку, кіберпростір можна розглядати як разючий глобальний спільний простір, який є легкодоступним, забезпечує високий ступінь зв'язку та здатний створити великі можливості для соціально-економічного зростання. З іншого боку, кіберпростір характеризується також слабкою юрисдикцією, труднощами приписувати дії, відсутністю кордонів і взаємопов'язаними системами, які можуть бути пористими, а дані з них можуть бути викрадені або навіть доступні іноземним урядам. На додаток до цих двох перспектив, цифрова екосистема відзначається концентрацією платформ та інфраструктури онлайн-сервісів у руках дуже малої кількості зацікавлених осіб. Усі вищезазначені аспекти спонукають країни-членів до підтримки й розвитку цифрового суверенітету. Досягнення цифрового суверенітету означає, що громадяни та бізнес можуть повною мірою досягати успіхів, використовуючи цифрові послуги та продукти ІКТ, які заслуговують на довіру, не хвилюючись ані за свої персональні дані, цифрові активи, економічну автономію, ані за політичний вплив.

Суверенітет даних або цифровий суверенітет відстоюється країнами-членами на національному та європейському рівнях. Хоча країни-члени, здається, не розглядають цю проблему безпосередньо у своїх національних стратегіях кібербезпеки як конкретну ціль, вони або розглядають її в рамках трансверсального принципу, або окреслюють свій намір забезпечити цифровий суверенітет на національному рівні в *спеціальних* публікаціях, зосереджуючись на ключових технологіях. Наприклад, у французькому стратегічному огляді кіберзахисту за 2018 рік зазначено, що "контроль за такими технологіями має першорядне значення для забезпечення цифрового суверенітету: шифрування зв'язку, виявлення кібератак, професійний мобільний радіозв'язок, хмарні обчислення та штучний інтелект"[37].

На європейському рівні країни-члени беруть активну участь у визначенні європейської стратегії щодо даних (COM/2020/66 кінцевий варіант) та побудові Керівництва ЄС з сертифікації цифрових продуктів, сервісів і процесів ІКТ, як це встановлено в Акті ЄС про кібербезпеку (2019/881), з метою забезпечення стратегічної цифрової автономії на європейському рівні.

Етап співбесід з країнами-членами показав, що тема цифрового суверенітету часто розглядається як ширше питання, аніж просто питання, яке обмежується кібербезпекою. Отже, країни-члени не висвітлюють цю тему у своїх національних стратегіях кібербезпеки, а для тих небагатьох, хто це робить, вони не охоплюють її як конкретну ціль *як таку*.

Забезпечити стимули для розвитку галузі кіберстрахування

Сучасний стан індустрії кіберстрахування свідчить про те, що світовий ринок безперечно виріс. Однак він все ще перебуває на початковій стадії, оскільки необхідно збирати дані та створювати багато прецедентів (*наприклад*, "мовчазний страховий захист", системні кібер-ризики тощо). Крім того, оцінені збитки, накопичені від кібератак у всьому світі, на кілька порядків перевищують поточний потенціал страхового покриття галузі кіберстрахування (робочий документ МВФ — Кіберризик для фінансового сектору: рекомендації для кількісної оцінки WP/18/143) . Однак розвиток галузі кіберстрахування, безумовно, може принести користь і закласти основу для доброчесних механізмів. Насправді механізми кіберстрахування можуть допомогти у:

- підвищенні обізнаності про ризики кібербезпеки в компаніях;
- кількісній оцінці впливу кіберризиків;
- вдосконаленні управління ризиками кібербезпеки;
- наданні підтримки організаціям, які стали жертвами кібератак; і
- покритті збитків (матеріальних або інших), спричинених кібератакою.

[37] http://www.sgdsn.gouv.fr/uploads/2018/03/revue-cyber-resume-in-english.pdf

Деякі країни-члени почали працювати над цією темою. Наприклад:

- Естонія застосувала підхід "чекай і спостерігай" у своїй Національній стратегії кібербезпеки: "Для пом'якшення кібер-ризиків загалом у приватному секторі будуть проаналізовані попит і пропозиція сервісів кіберстрахування в Естонії, і на цій основі будуть узгоджені принципи співпраці для пов'язаних сторін, у тому числі обмін інформацією, підготовка до оцінки ризику тощо. Сьогодні постачальників сервісів кіберстрахування на естонському ринку небагато, і спершу потрібно скласти мапу того, хто що пропонує. Складність страхового захисту часто вважається перешкодою для розвитку ринку кіберстрахування".
- Люксембург особливо підтримує розвиток галузі кіберстрахування у своїй Національній стратегії кібербезпеки: "Завдання 1: створення нових продуктів і сервісів. Для об'єднання ризиків і заохочення жертв цифрових кіберінцидентів звертатися за допомогою до експертів з метою управління інцидентом та відновлення системи, яка постраждала від зловмисної дії, страховим компаніям буде запропоновано створювати конкретні продукти для сфери кіберстрахування".

Відгуки опитаних на цю тему були досить різноманітними: деякі країни-члени заявили, що тема кіберстрахування нещодавно стала темою для обговорення, тоді як інші поділились тим, що хоча ця тема і є перспективною, галузь ще недостатньо дозріла для неї. Однак велика кількість опитаних заявили, що тема не розглядається як частина Національної стратегії кібербезпеки, або тому, що вона була визнана дуже конкретною, або не входить до сфери дії Національної стратегії кібербезпеки.

TP-06-20-047-EN-N

Про Європейське агентство з питань мережевої та інформаційної безпеки

Європейське агентство з питань мережевої та інформаційної безпеки, ENISA, є агентством Європейського Союзу, метою діяльності якого є досягнення високого загального рівня кібербезпеки в Європі. Засноване у 2004 році та у своїй діяльності підкріплене Законом ЄС про кібербезпеку, Європейське агентство з питань мережевої та інформаційної безпеки робить свій внесок у політику ЄС у сфері кібербезпеки, підвищує надійність продуктів, сервісів і процесів ІКТ (інформаційно-комунікаційних технологій) за допомогою схем сертифікації кібербезпеки, співпрацює з країнами-членами та органами ЄС і допомагає Європі підготуватися до кібервикликів майбутнього. Шляхом обміну знаннями, розбудови спроможності та підвищення обізнаності Агентство разом зі своїми ключовими зацікавленими особами працює заради зміцнення довіри до пов'язаної економіки, підвищення стійкості інфраструктури Союзу та, врешті-решт, для забезпечення цифрового захисту європейського суспільства та громадян. Більше інформації на сайті www.enisa.europa.eu.

ENISA
ЄВРОПЕЙСЬКЕ АГЕНТСТВО З ПИТАНЬ МЕРЕЖЕВОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Офіс в Афінах
вул. Васіліс Софіас, 1 (1 Vasilissis Sofias Str)
151 24 Марусі, Аттіка, Греція (151 24 Marousi, Attiki, Greece)

Офіс в Іракліоні
95 Ніколау Пластіре (95 Nikolaou Plastire)
700 13 Василіка Вутон, Іракліон, Греція (700 13 Vassilika Vouton, Heraklion, Greece)

enisa.europa.eu

ISBN: 978-92-9204-443-5
DOI: 10.2824/590072