Global
Cyber Security
Capacity Centre

Модель зрілості потенціалу кібербезпеки для націй

РЕДАКЦІЯ 2021

Резюме

Світова економіка продовжує розвиватись з дедалі більшою залежністю від технологій. Якщо не забезпечити наявність потенціалу кібербезпеки в усьому кіберпросторі, то неминуче буде створено кібергетто. В таких умовах збитки від кіберінцидентів можуть стати поширеним явищем, а самі кібератаки легко здійснити. Здатність країн реагувати та нарощувати потенціал перед обличчям мінливих загроз – будь то через тенденції у використанні технологій, соціально-політичний клімат чи еволюцію екосистеми суб'єктів загроз – ніколи не була такою важливою.

Модель зрілості потенціалу кібербезпеки для націй (CMM) допомагає країнам зрозуміти, що працює, що ні та чому, в усіх сферах потенціалу кібербезпеки. Це важливо для того, щоб уряди та підприємства мали змогу затвердити політику та здійснювати інвестиції, які потенційно можуть підвищити безпеку та захист у кіберпросторі, водночас поважаючи права людини, такі як конфіденційність і свобода слова.

З 2015 року Глобальний центр розвитку потенціалу в галузі кібербезпеки (Global Cyber Security Capacity Centre (GCSCC), Центр розвитку потенціалу) активно просуває CMM у різних секторах, задля обговорення можливостей кібербезпеки та сприяти вдосконаленню глобальних технологій. Прийняття CMM ключовими міжнародними зацікавленими сторонами, а також понад 120 проведених перевірок у більш ніж 85 країнах світу демонструє позитивний вплив дослідження, підтримує самооцінку уряду та інформує про розвиток галузевих інструментів і ресурсів.

Зважаючи на мінливий ландшафт загроз і відповідну практику кібербезпеки, GCSCC очолив перегляд CMM, перший з моменту виходу видання у 2016 році. Для підготовки цього видання 2021 року Центр розвитку потенціалу провів глобальну спільну роботу, спрямовану на отримання і синтез новітніх знань спільноти.

GCSCC розробив пропозиції щодо змін на основі досвіду, отриманого під час розгортання CMM, і провів серію онлайн і офлайн консультацій з експертами, щоб підтвердити висновки та обговорити зміни. Серед тих, з ким були проведені консультації, були Консультативна група експертів GCSCC, стратегічні, регіональні партнери та партнери з впровадження GCSCC, а також інші експерти з академічних установ, міжнародних і регіональних організацій, урядів, приватного сектору та громадянського суспільства. На основі їх вхідних даних були визначені, розроблені, уточнені та підтверджені показники для кожного Параметру.

Суб'єкти по всьому світу, починаючи від окремих осіб і закінчуючи державами, повинні гарантувати, що кіберпростір і системи, залежні від нього, є стійкими до зростаючих атак. Видання CMM 2021 та його застосування продовжать сприяти зусиллям, спрямованим на досягнення цієї стійкості, не лише шляхом отримання більш глибокого розуміння міжнародного потенціалу кібербезпеки, але і шляхом збільшення ефективних інвестицій у потенціал кібербезпеки на основі ретельного аналізу даних, зібраних під час розгортання моделі. Критичні прогалини в усіх сферах міжнародної кібербезпеки будуть виявлені та заповнені масштабованими та ефективними контрзаходами у співпраці з міжнародними партнерами з глобальної спільноти кібербезпеки.

Вдосконалення CMM не має статичного характеру; безперервний процес вдосконалення буде підтримуватися для забезпечення того, щоб CMM залишалась застосовною до всіх національних контекстів і відображала глобальний стан зрілості потенціалу кібербезпеки. Однак ця еволюція і надалі залишається продуманим процесом, стимульованим фактами і практикою.

Зміст

Національне оцінювання кібербезпеки з CMM

Огляд країни в рамках CMM передбачає збір даних командою дослідників, які проводять консультації із внутрішньодержавними зацікавленими сторонами. Результатом є підготовлений на основі фактичних даних звіт, який:

- визначає рівень зрілості потенціалу кібербезпеки країни;
- деталізує прагматичний набір заходів що сприятимуть усуненню прогалин у зрілості потенціалу кібербезпеки; та
- визначає пріоритети для інвестицій та майбутнього нарощування потенціалу на основі конкретних потреб країни.

Згідно з незалежним дослідженням, проведеним на замовлення Міністерства закордонних справ, у справах Співдружності та розвитку Великої Британії, переваги від CMM для країни є численними і включають:

- підвищення рівня обізнаності та розбудови потенціалу у сфері кібербезпеки, а також посилення співпраці в уряді;
- налагодження взаємодії та співпраці з бізнесом та суспільством в цілому;
- підвищення внутрішньої довіри до програми кібербезпеки в державних органах;
- допомога у визначенні ролей та обов'язків в уряді;
- надання доказів для збільшення фінансування розбудови потенціалу кібербезпеки; та
- основа для розробки стратегії та політики розвитку країни.

Важливо, щоб країна могла підтвердити свої досягнення у сфері кібербезпеки, а CMM визначає, якими мають бути ці докази та що вони демонструють. Такий збір доказів сам по собі є багатостороннім процесом із залученням широкого кола джерел та організацій. Дискусії можуть бути важливими для вирішення розбіжностей у думках. Чи будуть такі дискусії ефективними, якщо проводити їх дистанційно (і в режимі онлайн), або ж вони потребуватимуть особистих зустрічей, залежатиме від країни, яка проводить перевірку.

Для отримання додаткової інформації про методику перевірки CMM, процес і зразки звітів CMM: https://gcscc.ox.ac.uk/the-cmm

Параметри національного потенціалу кібербезпеки

CMM визначає, що кібербезпека складається з п’яти параметрів, які разом складають національний потенціал, необхідний країні для ефективного забезпечення кібербезпеки:

1. **Розробка політики та стратегії кібербезпеки;**
2. **Заохочення культури відповідального ставлення до кібербезпеки в суспільстві;**
3. **Підвищення рівня знань та навичок у сфері кібербезпеки;**
4. **Створення ефективної нормативно-правової бази; та**
5. **Управління ризиками за допомогою стандартів та технологій.**

Параметр 1 Політика та стратегія кібербезпеки досліджує спроможність країни розробляти та впроваджувати стратегію кібербезпеки, а також підвищувати її стійкість до кіберзагроз шляхом покращення реагування на інциденти, забезпечення кіберзахисту та захисту критичної інфраструктури (КІ). Цей параметр розглядає ефективну стратегію та політику у забезпеченні національної спроможності у сфері кібербезпеки, зберігаючи при цьому переваги кіберпростору, що є життєво важливими для уряду, бізнесу та суспільства в цілому.

Параметр 2 Культура та суспільство кібербезпеки розглядає важливі елементи, такі як розуміння ризиків, пов'язаних з кібербезпекою в суспільстві, рівень довіри до інтернет-сервісів, послуг електронного урядування та електронної комерції, а також розуміння користувачами питань захисту персональних даних в інтернет-просторі. Крім того, у цьому аспекті досліджується наявність механізмів звітності, що функціонують як канали для передачі користувачами повідомлень про кіберзлочини. Крім того, у ньому розглядається роль засобів масової інформації та соціальних мереж у формуванні цінностей, ставлення та поведінки у сфері кібербезпеки.

Параметр 3 Формування знань та можливостей у сфері кібербезпеки розглядає наявність, якість та розуміння програм для різних груп зацікавлених сторін, включаючи уряд, приватний сектор та населення в цілому, і стосується програм підвищення обізнаності щодо кібербезпеки, офіційних освітніх програм з кібербезпеки та програм професійної підготовки.

Параметр 4 Нормативно-правова база вивчає спроможність уряду розробляти та впроваджувати національне законодавство, яке прямо чи опосередковано стосується кібербезпеки, з особливим акцентом на питаннях регуляторних вимог до кібербезпеки, законодавства, пов'язаного з кіберзлочинністю, та пов'язаного з ним законодавства. Здатність забезпечувати виконання таких законів перевіряється за допомогою правоохоронних органів, прокуратури, регуляторних органів і суду. Крім того, розглядаються такі питання, як офіційні та неофіційні механізми взаємодії у боротьбі з кіберзлочинністю.

Параметр 5 Стандарти та технології стосуються ефективного та широкого використання технологій кібербезпеки для захисту окремих осіб, організацій та національної інфраструктури. У цьому Параметрі розглядається впровадження стандартів кібербезпеки та належної практики, розгортання процесів і засобів контролю, а також розробка технологій і продуктів для зменшення ризиків кібербезпеки.

CMM визначає п'ять етапів зрілості для всіх параметрів: початковий, формуючий, становлення, стратегічний та динамічний. Вони відповідають наступному: початковий розвиток потенціалу, становлення, світове лідерство, здатність передбачати та бути готовими до майбутніх потреб у сфері кібербезпеки.

Слід зазначити, що між параметрами існують зв'язки; наприклад, щоб бути ефективним в одній сфері потенціалу, часто висуваються вимоги до інших областей[1]. Справа також у тому, що ресурси обмежені, а пріоритети щодо посилення потенціалу, ймовірно, вимагатимуть відповідних заходів, які можуть охоплювати декілька параметрів. Таким чином, діяльність з порівняльного аналізу розглядає країну в контексті всієї CMM та за всіма параметрами, що дозволяє цілісно розглядати національний потенціал.

[1]Для того, щоб країна досягла встановленого рівня зрілості в рамках Параметру 3.1 «Ініціативи уряду» «Розбудова обізнаності про кібербезпеку», однією з вимог, яких необхідно дотримуватися, є те, що зміст скоординованої національної програми підвищення обізнаності про кібербезпеку включає чіткі посилання на національну стратегію кібербезпеки. Аналогічно, щоб країна досягла встановленого рівня зрілості в рамках Параметру 3.2 «Адміністрування» в освіті з кібербезпеки, пріоритети освіти з кібербезпеки, що виникають в результаті процесу консультацій з багатьма зацікавленими сторонами, повинні бути відображені в національній стратегії кібербезпеки.

Структура CMM

Параметр

П'ять параметрів разом охоплюють весь потенціал національної кібербезпеки, який оцінюється CMM. Кожен параметр включає низку чинників, які відображають основні компоненти потенціалу, необхідні для реалізації цього параметра. Разом вони представляють різні "лінзи", через які потенціал кібербезпеки може бути підтверджений і проаналізований.

Фактор

У рамках п'яти параметрів Фактори описують, що означає володіти потенціалом кібербезпеки. Це основні елементи національного потенціалу, які потім визначаються для етапі зрілості. Повний перелік факторів має на меті цілісно охопити всі потреби країни у сфері кібербезпеки. Більшість факторів складаються з ряду аспектів , які структурують показники фактора на більш стислі частини (які безпосередньо стосуються збору та аналізу даних). Однак, деякі Фактори , які є більш обмеженими за обсягом, не мають конкретних Аспектів.

Аспект

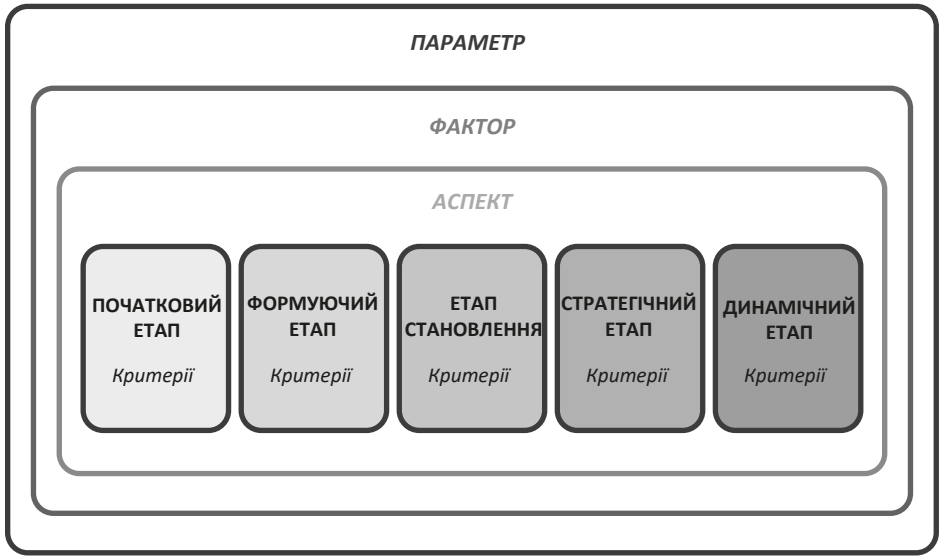
Якщо Фактор складається з декількох компонентів, то вони називаються Аспектами. Аспекти - це організаційний метод поділу показників на менші блоки, які легше зрозуміти. Кількість Аспектів залежить від тематики, що розкривається у змісті Фактора, та його загальної складності.

Етап

Етапи визначають ступінь прогресу країни по відношенню до певного фактора або аспекту потенціалу кібербезпеки. CMM складається з п'яти окремих етапів зрілості: початковий, формуючий, становлення, стратегічний, динамічний (докладніше на стор. 8). CMM порівнює країну з цими етапами, фіксуючи існуючий потенціал кібербезпеки, який країна може покращити або знизити залежно від вжитих дій (або бездіяльності). В рамках кожного Етапу існує ряд Критеріїв, які країна повинна виконати для успішного проходження Етапу.

Критерій

Критерії є основною частиною структури CMM. Кожен критерій описує кроки, дії або структурні елементи, які є показниками певного етапу зрілості. Для успішного досягнення Етапу зрілості країна повинна бути впевнена в тому, що вона може підтвердити кожен з критеріїв. Для підвищення зрілості потенціалу кібербезпеки країни необхідно домогтись відповідності всім Критеріям в рамках певного етапу. Більшість з цих критеріїв є бінарними за своєю природою, тобто країна може або підтвердити, що вона відповідає критеріям, або не може надати таких підтверджень.



Етапи розвитку національного потенціалу кібербезпеки

Етапи визначають ступінь прогресу країни по відношенню до певного фактора чи аспекту потенціалу кібербезпеки (див. стор. 7). Аналіз CMM буде порівнювати країну з цими етапами, враховуючи існуючий потенціал кібербезпеки.

Початковий

На даному етапі зрілості кібербезпеки або не існує, або вона має дуже примітивний характер. Можуть виникати початкові дискусії щодо розвитку потенціалу кібербезпеки, але без жодних конкретних дій. На цьому етапі можуть бути відсутні будь-які видимі докази;

Формуючий

Розпочинається розвиток та формулювання деяких особливостей аспекту, але вони можуть бути неорганізованими, погано визначеними або просто новими. Проте докази цієї діяльності можна чітко продемонструвати;

Становлення

Критерії Аспекту запроваджено, і факти свідчать про те, що вони працюють. Однак, не існує добре продуманого підходу до розподілу ресурсів. Було зроблено мало компромісних рішень щодо інвестицій у різні елементи Аспекту. Але Аспект є дієздатним і визначеним;

Стратегічний

Було зроблено вибір щодо того, які частини Аспекту є важливими, а які менш важливими для конкретної організації або нації. Стратегічний етап відображає той факт, що цей вибір був зроблений з урахуванням конкретних обставин, в яких перебуває країна або організація;

Динамічний

На цьому етапі існують чіткі механізми для внесення змін до національної стратегії залежно від існуючих обставин, таких як зміни в середовищі кіберзагроз, глобальний конфлікт або значні зміни в одній з проблемних сфер (наприклад, кіберзлочинність або конфіденційність). Існують також докази глобального лідерства з питань кібербезпеки. Ключові сектори, принаймні, розробили методи зміни стратегій на будь-якому етапі свого розвитку. Швидке прийняття рішень, перерозподіл ресурсів і постійна увага до мінливого середовища є особливостями цього етапу.

CMM дозволяє проводити порівняльний аналіз поточного національного потенціалу кібербезпеки. Розуміння вимог для досягнення більш високого рівня потенціалу безпосередньо вкаже на сфери для подальших інвестицій, і як підтвердити такі рівні потенціалу. CMM також можна використовувати для створення бізнес-кейсів для інвестицій і очікуваного підвищення продуктивності. Поєднання аналізу CMM з національними оцінками ризиків, соціальними та економічними стратегіями може сприяти подальшому визначенню пріоритетів щодо зміцнення потенціалу.

Параметр: 1 Політика та стратегія кібербезпеки

Цей параметр досліджує спроможність країни розробляти та впроваджувати стратегію кібербезпеки та підвищувати її стійкість до кіберзагроз шляхом покращення реагування на інциденти, забезпечення кіберзахисту та захисту критично важливої інфраструктури. Також тут розглядається ефективна стратегія та політика у забезпеченні національної обороноздатності у сфері кібербезпеки при збереженні переваг кіберпростору, що є життєво важливими для уряду, міжнародного бізнесу та суспільства в цілому.

Фактор
D1.1: Національна стратегія кібербезпеки

Стратегія кібербезпеки має важливе значення для інтеграції програми кібербезпеки в уряд, оскільки вона допомагає визначити пріоритетність кібербезпеки як важливої сфери політики, визначає обов'язки та повноваження ключових урядових і неурядових учасників, що займаються кібербезпекою, та спрямовує розподіл ресурсів на вирішення нових та існуючих проблем і пріоритетів у сфері кібербезпеки.

> Фактор

Аспекти

- **Розробка стратегії:** цей аспект стосується розробки національної стратегії, розподілу повноважень з її реалізації між секторами та цивільним суспільством, а також розуміння національних ризиків та загроз кібербезпеки, які зумовлюють зміцнення потенціалу на національному рівні;
- **Наповнення:** цей аспект стосується змісту національної стратегії кібербезпеки та того, чи вона прямо пов'язана з національними ризиками, пріоритетами та цілями, такими як національна безпека, підвищення обізнаності громадськості та пом'якшення кіберзлочинності, спроможність реагувати на інциденти та захист критичної важливої інфраструктури;
- **Впровадження та аналіз:** у цьому Аспекті розглядається наявність комплексної програми для координації кібербезпеки, включаючи власника департаменту або координуючий орган зі зведеним бюджетом;
- **Міжнародна взаємодія:** цей аспект досліджує, якою мірою країна обізнана про існування міжнародних дискусій щодо політики кібербезпеки, а також як міжнародні дебати щодо політики кібербезпеки та пов'язаних з нею питань впливають на інтереси та міжнародний статус країни.

Фактор
D 1.2: Реагування на інциденти та управління кризовими ситуаціями

Цей фактор стосується спроможності уряду систематично виявляти та визначати характерні ознаки інцидентів на національному рівні. Він також аналізує спроможність уряду організовувати, координувати та оперативно реагувати на інциденти, а також перевіряє, чи інтегрована кібербезпека в національну систему управління кризовими ситуаціями.

> Фактор

Аспекти

- **Ідентифікація та класифікація інцидентів:** цей аспект визначає, чи існують внутрішні механізми для ідентифікації та класифікації інцидентів;
- **Організація:** цей аспект стосується існування уповноваженого центрального органу, призначеного для збору інформації про інциденти, та його відносин з державним та приватним сектором для реагування на інциденти на національному рівні;
- **Інтеграція кібербезпеки в національну систему управління кризовими ситуаціями:** цей аспект досліджує, наскільки кібербезпека інтегрована в національну систему управління кризовими ситуаціями.

Фактор

D 1.3: Захист критичної інфраструктури (КІ)

Цей фактор вивчає здатність уряду ідентифікувати об'єкти критичної інфраструктури, нормативні вимоги, характерні для об'єктів критичної інфраструктури, та впровадження належної практики кібербезпеки операторами критичної інфраструктури.
> Фактор

Аспекти

- **Ідентифікація:** цей аспект стосується наявності загального переліку активів, секторів та операторів критичної інфраструктури, а також аудиту активів критичної інфраструктури на регулярній основі;
- **Нормативні вимоги:** цей аспект стосується наявності нормативних вимог, характерних для кібербезпеки критичної інфраструктури;
- **Експлуатаційна практика:** цей аспект досліджує, чи впроваджують оператори критичної інфраструктури визнані галузеві стандарти, а також наявність механізмів співпраці між та всередині секторів.

Фактор

D 1.4: Кібербезпека в сфері оборони та національної безпеки

Цей фактор досліджує, чи має уряд можливість розробляти та впроваджувати стратегію кібербезпеки в рамках національної безпеки та оборони. Він також розглядає рівень можливостей забезпечення кібербезпеки в структурі національної безпеки і оборони, а також механізми співпраці з питань кібербезпеки між цивільними та оборонними структурами.
> Фактор

Аспекти

- **Стратегія кібербезпеки в сфері оборони:** цей аспект стосується наявності стратегії підтримки кібербезпеки в рамках національної безпеки та оборони, а також того, чи підтримується вона відповідними правовими органами і відповідною оперативною доктриною і правилами застосування;
- **Спроможність сил оборони у сфері кібербезпеки:** у цьому Аспекті розглядається рівень спроможності у сфері кібербезпеки та організаційних структур у системі національної безпеки;
- **Координація цивільної оборони:** у цьому Аспекті розглядається співпраця з питань кібербезпеки між цивільними та оборонними структурами, а також наявність відповідних ресурсів.

Фактор - D1.1: Національна стратегія кібербезпеки

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Розробка стратегії	Національна стратегія кібербезпеки відсутня, але розпочато процес планування її розробки. Можливо, зверталися за порадою до міжнародних партнерів.	Розпочато процес розробки стратегії. Сформульовано загальний план/проект національної стратегії кібербезпеки. Узгоджено процеси консультацій з групами основних зацікавлених сторін, включаючи приватний сектор, громадського сектору та міжнародних партнерів.	Опубліковано національну стратегію кібербезпеки. Проведено оцінку ризиків національної кібербезпеки для конкретної країни. Стратегія відображає потреби та ролі відповідних зацікавлених сторін в уряді, бізнесі та суспільстві. Існує програма впровадження, яка охоплює сферу дії стратегії. Існують механізми, які дозволяють "власникам" стратегії контролювати отримані результати, вирішувати питання впровадження та підтримувати узгодженість стратегії.	Налагоджено процеси перегляду та оновлення стратегії. Нові ризики в сфері кібербезпеки регулярно оцінюються та використовуються для оновлення стратегії та плану впровадження. Вплив стратегії на зменшення ризиків та шкоди є зрозумілий і використовується для обґрунтування фінансування та пріоритетних рішень.	Національна стратегія кібербезпеки та план її впровадження активно переглядаються з метою врахування більш масштабних стратегічних змін у країні (політичних, економічних, соціальних, технічних, правових та екологічних). Країна є визнаним авторитетом у світовій спільноті і підтримує розвиток національних і глобальних стратегій кібербезпеки. Питання кібербезпеки включені в інші відповідні стратегії та програми впровадження на національному рівні.
Наповнення	Можуть існувати різні національні політики та стратегії, які стосуються кібербезпеки, але вони не є повними і практично немає доказів того, що вони відображають конкретні національні пріоритети та умови.	Існує матеріал, який відображає пріоритети та умови конкретної країни. Існує зв'язок між стратегією (або проектом стратегії) та пріоритетами такими як національна безпека, цифрова стратегія та економічний розвиток, але вони є як правило, носять ситуативний характер і їм бракує деталізації. Стратегія (або проект стратегії) визначає основні результати, за якими можна оцінити досягнення.	Зміст національної стратегії кібербезпеки базується на комплексній оцінці ризиків, яка включає чіткі зв'язки з більш широкою економічною та політичною діяльністю і стратегіями на національному рівні. Зміст включає в себе заходи, спрямовані на підвищення обізнаності суспільства та бізнесу, протидії кіберзлочинності створення можливостей реагування на інциденти, сприяння державно-приватному партнерству та захист критичної інфраструктури та економіки в цілому. Розглянуто як національна стратегія кібербезпеки може включати або підтримувати ширші цілі Інтернет-політики, такі як: захист дітей; захист прав людини; захист рівності, різноманітності та інклюзивності; і боротьба з дезінформацією.	У змісті враховано вплив на ризики кібербезпеки нових технологій та їх використання у критичній інфраструктурі, економіці та суспільстві. Результати, визначені у стратегії, є конкретними та вимірюваними. Визначено метрики, які дозволяють зацікавленим сторонам оцінювати ефективність стратегії щодо зниження заподіяної шкоди. Розглянуто питання щодо того, яким чином позитивні результати впровадження стратегії можуть бути збережені після закінчення терміну її дії, в тому числі, яким чином буде фінансуватися підтримка нових можливостей.	Зміст враховує вплив більш масштабних подій на ризики кібербезпеки (політичні, економічні, соціальні, технічні, правові та екологічні). Зміст національної стратегії кібербезпеки сприяє та заохочує двостороннє та багатостороннє співробітництво між країнами з метою забезпечення безпечного, стійкого та надійного кіберпростору.

Фактор - D1.1: Національна стратегія кібербезпеки

Аспект	Початковий	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Впровадження та аналіз	Не розроблено жодної програми впровадження національної кібербезпеки	Розробляється комплексна програма впровадження кібербезпеки із залученням відповідних зацікавлених сторін, включно з приватним сектором та цивільним суспільством. Заходи в рамках програми були закріплені за конкретними "виконавцями", але наявність необхідних ресурсів ще не підтверджена. Механізми контролю процесів обмежені або несистематичні.	Оприлюднено детальний план впровадження, що включає заходи, відповідальних осіб та фінансові ресурси. План впровадження передбачає залучення відповідних зацікавлених сторін з державного та інших секторів. Призначено координаційний орган. Орган має достатньо повноважень, щоб забезпечити притягнення до відповідальності "винуватців" дій. Ресурси, необхідні для виконання заходів програми, визначені та доступні. Виявляється нестача бюджетних коштів та інформується відповідний орган влади. Впроваджено процеси перевірки програм та показників, які дозволяють оцінювати прогрес та інформувати відповідні органи влади про ризики, проблеми та залежності. Ці процеси фінансуються належним чином.	Для моніторингу впливу програми на зниження ризиків (та інші відповідні цілі стратегії) використовуються показники, орієнтовані на результат. Існують підтвердження того, що ці показники використовуються для вдосконалення плану подальших заходів. Показники (як прогрес, так і показники, орієнтовані на результат) беруться з широкого кола державних, недержавних та міжнародних джерел. Існує незалежний контроль та/або гарантія виконання програми.	Створено механізми для внесення більш суттєвих змін до програми у разі істотних змін обставин (політичних, економічних, соціальних, технічних, правових та екологічних). Програма сприяє глобальному розвитку показників, орієнтованих на результат, та їх використанню.
Міжнародна взаємодія	Існує обмежена обізнаність про основні міжнародні дискусії, що стосуються політики кібербезпеки (таких як норми кібербезпеки, взаємна правова допомога, управління Інтернетом, суверенітет та захист даних) Країна може отримати користь від регіональних/міжнародних мереж оперативної співпраці, але не бере в них активної участі.	Країна усвідомлює існування міжнародних дискусій щодо політики кібербезпеки та пов'язаних з нею питань. Країна може іноді брати участь у регіональних або міжнародних дискусіях з питань, пов'язаних з кібербезпекою, але загалом не приймає в них активної участі. Країна може брати участь у відповідних органах оперативної співпраці та політики (таких як FIRST*, регіональні органи CERT**, IGF*** або UNGGE****), але здебільшого дотримується пасивної позиції.	Оцінено вплив міжнародних дискусій щодо політики кібербезпеки та пов'язаних з нею питань на інтереси та міжнародний статус країни. Відповідно, були визначені конкретні цілі взаємодії. До цього процесу було залучено багато зацікавлених сторін. Країна бере активну участь у роботі відповідних міжнародних органів та форумів як безпосередньо, так і через відповідні представницькі органи. Їхні думки чують і вони мають вплив. Країна робить активний внесок у регіональну/міжнародну оперативну співпрацю та політичні органи.	Країна активно формує міжнародне партнерство навколо конкретних цілей політики у сфері кібербезпеки та сприяє їх прийняттю. Країна робить значний внесок у регіональні/міжнародні оперативні органи та бере активну участь у розвитку потенціалу в інших країнах.	Країна є провідним учасником у досягненні консенсусу, сприянні інклюзивності та формуванні міжнародних дискусій з ключових питань політики у сфері кібербезпеки. Країна орієнтована на майбутнє, бачить нові проблеми (навколо нових технологій або нових видів загроз) та ініціює нові міжнародні дискусії навколо важливих питань. Країна бере активну участь у створенні нових регіональних/міжнародних механізмів співпраці.

* Форум груп реагування на інциденти та безпеки
** Група реагування на комп 'ютерні надзвичайні ситуації
*** Форум з питань управління Інтернетом
**** Група урядових експертів Організації Об 'єднаних Націй

Фактор - D 1.2: Реагування на інциденти та управління кризовими ситуаціями

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Ідентифікація та класифікація інцидентів	Процедури ідентифікації та класифікації інцидентів на національному рівні не існує.	Деякі організації та сектори мають внутрішні механізми для виявлення та класифікації інцидентів у межах своєї компетенції. Розробляється процес ідентифікації інцидентів на національному рівні. Не існує центрального реєстру, але існують спеціальні механізми для реєстрації найважливіших подій.	Більшість великих організацій мають внутрішні механізми для виявлення та класифікації інцидентів. Існує центральний реєстр інцидентів кібербезпеки національного рівня та запроваджено процес оперативного інформування про інциденти, починаючи з організаційного і закінчуючи національним рівнем. Окремі національні інциденти класифікуються за ступенем тяжкості і відповідно до цього виділяються ресурси	Висновки, що зроблені в результаті обробки інцидентів на національному рівні, регулярно аналізуються з метою винесення уроків та формування більш широкої політики і стратегії кібербезпеки.	Критерії класифікації інцидентів є достатньо гнучкими для того, щоб врахувати швидкоплинні зміни у технологічному середовищі або характері загроз. Країна сприяє впровадженню найкращих міжнародних практик у сфері ідентифікації та категоризації інцидентів.
Організація	Організації для реагування на кіберінциденти на національному рівні не існує. Деякі організації мають внутрішні механізми реагування на інциденти у сфері кібербезпеки, але їхня координація є мінімальною.	Національний CERT* може існувати, але не має достатніх ресурсів та навичок. Процеси управління інцидентами все ще перебувають на стадії розробки. Деякі організації державного та приватного секторів мають внутрішні механізми реагування на інциденти у сфері кібербезпеки, але їхня співпраця з національним CERT є несистематичною. Роль субнаціональних органів незрозуміла. Двостороннє співробітництво з міжнародними партнерами має обмежений або несистемний характер.	Створено національний орган з реагування на інциденти. Він має ресурси, навички, задокументовані процеси та юридичні повноваження, необхідні для реагування на різноманітні сценарії кіберінцидентів, з якими може зіткнутися країна (у тому числі, за необхідності, у неробочий час). Взаємовідносини та протоколи існують для забезпечення координації управління інцидентом між національним органом та іншими елементами державного та приватного секторів. Роль субнаціональних органів у реагуванні на інциденти є чіткою і створені механізми для забезпечення координації між національним та субнаціональним рівнями. Між національним органом та широким загалом організацій державного та приватного секторів, а також міжнародними партнерами відбувається регулярний обмін інформацією про загрози та вразливості, а також передовим досвідом роботи.	Національний орган здійснює широкий спектр заходів, таких як створення спільнот за інтересами, проведення міжгалузевих навчань та просування найкращих практик кібербезпеки. Національний орган впроваджує нововведення для надання ряду додаткових послуг, які покращують спроможність країни запобігати, виявляти, реагувати на інциденти та відновлюватися після реалізованих загроз. Національний орган визнаний як авторитетний представник з питань кібербезпеки в країні. Ефективність національного органу у питаннях зниження кібер-ризиків та завданої шкоди регулярно оцінюється та порівнюється з міжнародними передовими практиками.	Загальне оперативне реагування уряду є пристосованим до змін у технічному середовищі та характері загроз. Країна робить свій внесок у передовий міжнародний досвід організації оперативного реагування на загрози кібербезпеці.

* Група реагування на комп 'ютерні надзвичайні ситуації

Фактор - D 1.2: Реагування на інциденти та управління кризовими ситуаціями

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Інтеграція кібербезпеки в національну систему управління кризовими ситуаціями	Не існує системи управління кризовими ситуаціями на національному рівні. Кібербезпека не розглядалася як потенційний сценарій кризи на національному рівні. Можливості зв'язку в надзвичайних ситуаціях обмежені.	Національна система управління кризовими ситуаціями перебуває на стадії розробки, і на конкретну організацію покладено відповідальність за керівництво реагуванням на кризові ситуації на національному рівні. Кібербезпека визнана важливою складовою національного управління кризовими ситуаціями, як самостійний фактор, так і елемент інших кризових сценаріїв. Розробляється програма навчань, яка включатиме сценарії з кібербезпеки. Можливості зв'язку в надзвичайних ситуаціях існують, але вони можуть бути недостатньо інтегровані або не мати стійкості до кібератак.	Кібербезпека повністю інтегрована в національну систему управління кризовими ситуаціями, а організація, відповідальна за управління кризовими ситуаціями, здатна реагувати на різноманітні сценарії, пов'язані з кібербезпекою. Роль органу з управління кіберінцидентами в процесі врегулювання кризових ситуацій чітко визначена та встановлена, а порогові значення ескалації повністю зрозумілі. Регулярно відпрацьовуються національні сценарії врегулювання кризових ситуацій з елементами кібербезпеки. Системи екстреного зв'язку регулярно тестуються на кіберстійкість до різних сценаріїв, пов'язаних з інцидентами у сфері кібербезпеки.	Уроки, отримані під час навчань з подолання кризових ситуацій в сфері кібербезпеки, використовуються як для формування національної політики врегулювання кризових ситуацій, так і для розробки національної стратегії кібербезпеки та плану її впровадження. Існує міжнародне кризове планування та навчання з партнерами, які регулярно включають кібербезпеку як елемент. Стійкість систем зв'язку в надзвичайних ситуаціях була протестована за допомогою стрес-тестів на основі широкого спектру потенційних сценаріїв.	Країна робить свій внесок у дискусії щодо інтеграції кіберу в національне та міжнародне управління кризовими ситуаціями. Засоби зв'язку в надзвичайних ситуаціях здатні функціонувати за межами державного кордону з метою підтримки інших країн та реагування на глобальні кризові ситуації.

Фактор - D 1.3: Захист критичної інфраструктури (КІ)

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Ідентифікація	Можливо, є певне розуміння того, що є активом КІ, але не існує формальної класифікації активів КІ не було створено.	Створено перелік основних активів, секторів та операторів КІ.	Перелік об'єктів КІ був формалізований і включає низку відповідних організацій державного та приватного секторів. Визначено конкретних операторів, які знають про свій статус. Перелік постійно оновлюється з метою відображення змін у ситуації в країні. Виявлено транскордонні залежності.	Перелік активів КІ є адаптивним до стратегічних змін у технічному, соціальному та економічному середовищі. Здійснюється управління взаємозалежностями між секторами. Здійснюється управління транскордонними залежностями.	Процес виявлення активів КІ є гнучким, що дозволяє враховувати швидкі зміни в технологічному середовищі або загрозах. Країна бере активну участь у виявленні та визначенні пріоритетності глобальних активів КІ. Зменшується міжгалузева та транскордонна залежність.
Нормативні вимоги	Відсутні регуляторні вимоги, що стосуються кібербезпеки КІ.	Визнається потреба в базових стандартах для управління активами КІ, але вони не визначені в законодавстві. Галузеві регулюючі органи зазвичай не оцінюють операторів КІ на предмет відповідності вимогам.	Оператори КІ зобов'язані дотримуватися встановлених стандартів кібербезпеки (або у формі спеціального кіберрегулювання, або як частину більш широких регуляторних вимог). Запроваджено обов'язкові вимоги щодо звітування про зломи та виявлені вразливості. Впроваджено формальні процеси для оцінки дотримання оператором КІ нормативних стандартів, і виявлення інцидентів та вразливостей.	Розробляються нові підходи для регуляторного контролю з метою покращення кібербезпеки КІ, а також сприяння ефективному та якісному наданню послуг з питань КІ. Країна популяризує передові практики регулювання на міжнародному рівні.	Нормативно-правова база є достатньо гнучкою для того, щоб відповідати швидким змінам у технологічному середовищі чи характері загроз. Країна бере активну участь у формуванні нормативно-правових підходів до забезпечення глобальної КІ.
Експлуатаційна практика	Деякі оператори КІ можуть впроваджувати передові практики кібербезпеки , але вони є суперечливими.	Багато операторів КІ впроваджують передові практики кібербезпеки. Існує певна самооцінка за визнаними галузевими стандартами. Існують певні неформальні домовленості щодо співпраці між секторами та всередині секторів.	Оператори КІ послідовно впроваджують загальновизнані галузеві стандарти, а ефективність заходів контролю кібербезпеки регулярно оцінюється. Існують механізми, що дозволяють операторам обмінюватися інформацією про загрози та вразливості, кращими практиками та досвідом, отриманим в результаті інцидентів та помилок. Оператори КІ беруть повноцінну участь у плануванні та проведенні національних навчань з реагування на інциденти кібербезпеки та управління кризовими ситуаціями. Існують механізми надання органами державної влади інформаційної та іншої практичної підтримки операторам КІ як до, так і після інциденту.	Налагоджено активну співпрацю між операторами КІ та органами державної влади з метою розробки стратегій, що сприяють зміцненню колективної кібербезпеки. Стійкість екосистеми критичної інфраструктури в цілому оцінено за низкою сценаріїв, запроваджено заходи для усунення системних ризиків в економіці та суспільстві.	Країна та її оператори КІ роблять свій внесок у міжнародні переговори щодо захисту глобальної критичної інфраструктури. Експерти контролюючих органів та операторів КІ визнані на міжнародному рівні за їхній внесок у вирішення глобальних проблем захисту інфраструктури.

Фактор - D 1.4: Кібербезпека в сфері оборони та національної безпеки

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Стратегія кібербезпеки в сфері оборони	Потенційний вплив кібербезпеки на національну безпеку і оборону, можливо, розглядався, але не був офіційно зафіксований.	Проведено оцінку потенційного впливу кібербезпеки на національну безпеку і оборону та розробляється стратегія протидії цим ризикам. Цей аналіз включає ризики щодо можливостей військових та інших активів національної безпеки країни діяти у складному кіберпросторі.	Офіційно прийнято стратегію кібербезпеки для національної безпеки і оборони (як окремий документ або як частину більш широкого документу). Стратегія підкріплена відповідними юридичними повноваженнями та відповідною оперативною доктриною і практиками. Це узгоджується з міжнародним гуманітарним правом. Залежність суб'єктів національної безпеки і оборони від кібербезпеки інших частин критичної інфраструктури зрозуміла і врахована в оборонній стратегії кібербезпеки. Питання кібербезпеки впливають на інші елементи національної стратегії безпеки і оборони, де це доцільно.	Стратегія оборони включає відповідні заходи стримування. Міністерство оборони і національної безпеки країни (поряд з іншими зацікавленими сторонами) бере активну участь у глобальній дискусії щодо міжнародного гуманітарного права та норм поведінки, які стосуються конфліктів у кіберпросторі. Декларативна стратегія та оприлюднена доктрина можуть бути частиною цього процесу.	Стратегія і доктрина не є статичними, вони адаптуються до змін у спроможностях, геополітичному та технічному середовищі загроз. Стратегія призначена для забезпечення стабільності в кіберпросторі. Це включає заходи з прогнозування та впливу на стратегії, дії та реакції потенційних союзників і супротивників.
Спроможність сил оборони у сфері кібербезпеки	Потенціал фахівців у сфері кібербезпеки в структурі національної безпеки є обмеженим.	Вимоги до фахівців у сфері кібербезпеки є зрозумілими, а відповідні структури визначені. Зроблено перші кроки для їх створення.	Ресурси та організаційні структури вже створені та перевірені. Ресурси надаються через національний військовий кошторис або аналогічний процес. Оперативна доктрина та правила взаємодії повністю включені у навчання. Для надання підтримки застосовуються спеціалізовані розвідувальні засоби, які забезпечені відповідними ресурсами. Механізми сприяння співробітництву з союзниками створені та перевірені на практиці.	Існують відповідні механізми стримування та оборони/ стійкості, що є частиною оборонної стратегії кібербезпеки країни. Кібербезпека включена до більш масштабної оперативної та командної підготовки збройних сил країни.	Оборонні можливості кібербезпеки здатні підтримувати багатосторонні відповіді на загальні виклики національній безпеці.

Фактор - D 1.4: Кібербезпека в сфері оборони та національної безпеки

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Координація цивільної оборони	Співпраця у сфері кібербезпеки між цивільними та оборонними структурами обмежена.	Неформальна співпраця з питань кібербезпеки між цивільними та оборонними структурами може існувати, але не була формалізована. Оборонні відомства офіційно не були забезпечені ресурсами для проведення цієї роботи.	Співпраця у сфері кібербезпеки між цивільними та оборонними структурами існує та формалізована. Відповідні функції були визначені в рамках процедур управління кризовими ситуаціями в країні. Ресурси, необхідні в оборонній і національній спільноті безпеки, для підтримки цивільних і державних органів, були оцінені і розподілені на офіційному рівні. Існують формальні механізми для визначення військової/національної безпеки залежностей кібербезпеки від цивільної інфраструктури та КІ. Забезпечено спроможність операторів цивільної інфраструктури та інфраструктури КІ надавати ці послуги.	Співпраця цивільної оборони з питань кібербезпеки вбудована в стратегічне планування обох секторів і призначена для врегулювання низки майбутніх кризових сценаріїв. Існують механізми, які дозволяють оборонній спільноті та сектору національної безпеки використовувати навички та можливості економіки та суспільства в цілому.	Країна очолює міжнародні дебати щодо найкращих практик міжурядової співпраці у сфері кібербезпеки між цивільним та оборонним секторами.

Параметр 2: Культура та суспільство кібербезпеки

Цей параметр розглядає важливі елементи свідомої культури кібербезпеки, такі як розуміння суспільством ризиків, пов'язаних з кіберпростором, рівень довіри до інтернет-послуг, електронного урядування та електронної комерції, а також розуміння користувачами захисту персональних даних в Інтернеті. Крім того, у цьому компоненті досліджується наявність механізмів звітності, що функціонують як канали для користувачів, через які вони можуть повідомляти про кіберзлочини. Крім того, у ньому розглядається вплив засобів масової інформації та соціальних мереж на формування цінностей, ставлення та поведінки у сфері кібербезпеки.

Фактор
D 2.1: Уявлення про кібербезпеку

Цей фактор оцінює наскільки кібербезпека є пріоритетною та інтегрованою в цінності, підходи та практики державних органів, приватного сектору та користувачів в цілому. Уявлення про кібербезпеку складаються з цінностей, поглядів і практик, в тому числі звичок окремих користувачів, експертів та інших учасників екосистеми кібербезпеки, що підвищують здатність користувачів захищати себе в мережі Інтернет.
> Фактор

Аспекти

- **Усвідомлення ризиків:** цей аспект вивчає рівень усвідомлення ризиків кібербезпеки в державних органах, приватному секторі та серед користувачів;
- **Пріоритет безпеки:** в цьому Аспекті розглядається наскільки державні органи, приватний сектор та користувачі вважають питання кібербезпеки пріоритетними; та
- **Практика:** у цьому Аспекті розглядається, чи дотримуються державні органи, приватний сектор та користувачі принципів кібербезпеки.

Фактор
D 2.2: Рівень довіри та впевненості в онлайн-послугах

Цей фактор розглядає критичні навички, управління дезінформацією, рівень довіри та впевненості користувачів у використанні онлайн-послуг загалом та послуг електронного урядування та електронної комерції зокрема.
> Фактор

Аспекти

- **Навички цифрової грамотності:** цей аспект досліджує, наскільки користувачі критично оцінюють те, що вони бачать або отримують в Інтернет-мережі;
- **Довіра користувачів до пошуку інформації в Інтернеті:** цей аспект досліджує, чи користувачі впевнені в безпечності використання Інтернету на основі показників надійності сайтів;
- **Дезінформація:** у цьому Аспекті розглядається наявність інструментів та ресурсів для протидії дезінформації в Інтернеті;
- **Довіра користувачів до Державних електронних послуг:** цей Аспект вивчає, чи пропонуються державні електронні послуги, чи існує довіра до безпечного надання таких послуг, і чи докладаються зусилля для підвищення довіри шляхом впровадження заходів безпеки; а також
- **Довіра користувачів до онлайн-послуг:** цей аспект досліджує, чи пропонуються та надаються послуги онлайн-послуг у безпечному середовищі та чи користуються вони довірою з боку споживачів.

Фактор
D 2.3: Розуміння користувачем питань захисту персональних даних в Інтернеті

Цей фактор розглядає, чи визнають та розуміють користувачі Інтернету та зацікавлені сторони в державному та приватному секторах важливість захисту персональних даних в Інтернеті, а також чи усвідомлюють вони свої права на недоторканність приватного життя.
> Фактор

Аспекти

- **Захист персональних даних в Інтернеті:**
  (як зазначалося вище)

Фактор
D 2.4: Механізми звітування

Цей фактор досліджує наявність механізмів звітності, які функціонують як канали для користувачів, через які вони можуть повідомляти про інтернет-злочини, такі як онлайн-шахрайство, кібербулінг, насильство над дітьми в Інтернеті, викрадення персональних даних, порушення конфіденційності та системи безпеки, а також інші інциденти.
> Фактор

Аспекти

- **Механізми звітування:**
  (як зазначено вище)

Фактор
D 2.5: Медіа та онлайн-платформи

Цей фактор досліджує, чи є кібербезпека предметом дискусій в медійному просторі, а також темою для обговорення в соціальних мережах. Крім того, цей фактор розглядає роль медіа у поширенні інформації про кібербезпеку серед суспільства, формуючи таким чином його цінності, ставлення до кібербезпеки та поведінку в Інтернеті.
> Фактор

Аспекти

- **Засоби масової інформації та соціальні мережі:**
  (як зазначено вище)

Фактор - D 2.1: Уявлення про кібербезпеку

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Усвідомлення ризиків	Уряд має мінімальний рівень розуміння ризиків кібербезпеки або взагалі не розуміє їх. Приватний сектор має мінімальний рівень розуміння ризиків кібербезпеки або взагалі не усвідомлює їх. Рівень розуміння користувачами ризиків кібербезпеки є мінімальним або взагалі відсутній.	Провідні державні установи мають мінімальний рівень розуміння ризиків кібербезпеки. Провідні приватні компанії мають мінімальний рівень розуміння ризиків кібербезпеки. Незначна кількість інтернет-користувачів усвідомлюють ризики кібербезпеки.	У більшості державних установ існує розуміння ризиків кібербезпеки. У більшості приватних компаній існує розуміння ризиків кібербезпеки. Все більша кількість користувачів Інтернету в суспільстві усвідомлюють ризики кібербезпеки.	Державні органи всіх рівнів усвідомлюють ризики кібербезпеки та активно прогнозують нові ризики. Суб'єкти приватного сектору всіх рівнів повністю усвідомлюють ризики кібербезпеки та готуються до нових ризиків. Користувачі повністю усвідомлюють ризики кібербезпеки та намагаються передбачати нові ризики.	Державні установи всіх рівнів повністю усвідомлюють ризики кібербезпеки та використовують їх для оновлення політики та оперативних практик у сфері кібербезпеки. Більшість суб'єктів приватного сектору всіх рівнів зменшують ризики кібербезпеки та використовують їх для оновлення політики та оперативних практик у сфері кібербезпеки. Більшість користувачів ідентифікують та попереджають ризики кібербезпеки та намагаються адаптувати свою поведінку.
Пріоритет безпеки	Уряд мінімально або взагалі не визнає необхідність пріоритетності кібербезпеки. Суб'єкти приватного сектору мають мінімальне усвідомлення або взагалі не визнають необхідність надання кібербезпеці пріоритетного значення. Користувачі мають мінімальне усвідомлення або взагалі не усвідомлюють необхідності визначення пріоритетності кібербезпеки. Не існує жодних опитувань чи показників для документування кібербезпеки в уряді, приватному секторі або серед користувачів.	Провідні державні установи та приватні компанії визнають необхідність надання кібербезпеці пріоритетного значення. Приватні компанії визнають необхідність надання пріоритету кібербезпеці. Незначна кількість інтернет-користувачів визнає необхідність надання кібербезпеці пріоритетного значення. Опитування та показники для оцінки знань з кібербезпеки в країні обмежені або несистематичні.	Більшість державних органів всіх рівнів визначають кібербезпеку своїм пріоритетом. Більшість приватних компаній всіх рівнів визначають кібербезпеку своїм пріоритетом. Зростаюча кількість інтернет-користувачів у суспільстві визначає кібербезпеку своїм пріоритетом. В країні існують опитування та заходи для оцінки знань з кібербезпеки.	Державні органи всіх рівнів регулярно визначають та переоцінюють пріоритети кібербезпеки у відповідь на зміни загроз для населення. Більшість суб'єктів приватного сектору всіх рівнів регулярно визначають та переоцінюють пріоритети кібербезпеки у відповідь на зміни загроз для населення. Більшість користувачів регулярно надають кібербезпеці пріоритетне значення та прагнуть вживати активних заходів для покращення кібербезпеки. Регулярно проводяться опитування, які оприлюднюються в державних установах, бізнесі та промисловості, а також серед користувачів, та надаються відповідні показники.	Державні установи всіх рівнів зазвичай ставлять кібербезпеку в пріоритет як само собою зрозуміле питання. Зазвичай, суб'єкти приватного сектору всіх рівнів вважають кібербезпеку своїм пріоритетом. Користувачі звикли ставити кібербезпеку в пріоритет і вживають заходів для підвищення рівня своєї безпеки в Інтернеті. Результати опитування використовуються для вдосконалення політики кібербезпеки, інформування оперативної практики та ініціатив, пов'язаних з IT в країні.
Практика	Державні органи не дотримуються безпечних практик кібербезпеки. Приватні компанії не дотримуються безпечних практик кібербезпеки. В країні дуже мало інтернет-користувачів дотримуються безпечних практик кібербезпеки або вживають захисних заходів для забезпечення своєї безпеки.	Провідні державні установи дотримуються безпечних практик кібербезпеки. Провідні приватні фірми дотримуються безпечних практик кібербезпеки. Невелика, але зростаюча кількість інтернет-користувачів знає або дотримується безпечних практик кібербезпеки.	Більшість державних установ всіх рівнів дотримуються безпечних практик кібербезпеки. Більшість приватних компаній всіх рівнів дотримуються безпечних практик кібербезпеки. Більшість користувачів Інтернету в країні знають і дотримуються безпечних практик кібербезпеки	Державні установи всіх рівнів регулярно дотримуються безпечних практик кібербезпеки. Більшість суб'єктів приватного сектору всіх рівнів регулярно дотримуються безпечних практик кібербезпеки. Більшість користувачів знають і регулярно дотримуються безпечних практик кібербезпеки.	Державні органи всіх рівнів звикли дотримуватися, а також розвивати безпечні практики кібербезпеки. Суб'єкти приватного сектору всіх рівнів звикли дотримуватися та розвивати безпечні практики кібербезпеки. Майже всі користувачі знають і звикли дотримуватися безпечних практики кібербезпеки як само собою зрозуміле.

Фактор - D 2.2: Рівень довіри та впевненості в онлайн-послугах

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Навички цифрової грамотності	Дуже мало інтернет-користувачів в країні критично оцінюють те, що вони бачать або отримують в Інтернеті. Користувачі Інтернету, як правило, не вірять або навіть не підозрюють, що вони мають можливість користуватися Інтернетом та захищати себе в мережі. Немає програм для підтримки навичок цифрової та медіаграмотності.	Обмежена, але зростаюча кількість інтернет-користувачів критично оцінює те, що вони бачать або отримують в Інтернеті. Незначна кількість вірить, що вони мають можливість користуватися Інтернетом та захищати себе в мережі. Розробляються одна або кілька програм для підтримки навичок цифрової та медіаграмотності.	Більшість інтернет-користувачів критично оцінюють те, що вони бачать або отримують в Інтернеті, спираючись на виявлення можливих ризиків. Більшість інтернет-користувачів розуміють, як захистити себе від дезінформації в Інтернеті, наприклад, під час пошуку, і діють відповідно до цього. Були розроблені програми для підтримки навичок цифрової та медіаграмотності.	Більшість інтернет-користувачів критично оцінюють те, що вони бачать або отримують в Інтернеті, спираючись на виявлення можливих ризиків. Більшість інтернет-користувачів розпізнають сумнівну інформацію в Інтернеті та вживають заходів для її ігнорування або перевірки її достовірності. Докладаються зусилля для координації програм, спрямованих на підтримку навичок інтернет-, цифрової та медіаграмотності, між провайдерами інтернет-платформ, регуляторними органами та суспільством.	Майже всі користувачі звикли оцінювати ризики при користуванні інтернет-послугами, в тому числі з урахуванням змін у технічному та кібербезпековому середовищі. Користувачі Інтернету постійно коригують свою поведінку на основі оцінки якості інформації, яку вони отримують. Провайдери інтернет-платформ, регуляторні органи та суспільство спільно розробляють програми для розвитку навичок інтернет-, цифрової та медіаграмотності.
Довіра користувачів до пошуку інформації в Інтернеті	Більшість користувачів не довіряють або сліпо довіряють сайтам і тому, що вони бачать або отримують в Інтернеті. Дуже мало інтернет-користувачів відчувають себе безпечно при користуванні Інтернетом. Опитування або інші показники для оцінки довіри та безпеки користувачів в Інтернеті відсутні.	Лише незначна кількість користувачів має достатній рівень довіри до використання Інтернету. Незначна кількість інтернет-користувачів відчуває себе безпечно, користуючись Інтернетом. Опитування та показники для оцінки довіри та безпеки користувачів в Інтернеті обмежені або несистематичні.	Збільшується кількість користувачів, які мають достатній рівень довіри до безпечного користування Інтернетом та розпізнають індикатори безпечних сайтів та джерел інформації. Все більше користувачів відчувають себе безпечно, користуючись Інтернетом. Опитування та показники для оцінки довіри та впевненості користувачів в Інтернеті впроваджені та належним чином фінансуються.	Більшість користувачів мають сформований рівень довіри до безпечного користування Інтернетом та розпізнають індикатори легітимних сайтів та джерел інформації. Більшість користувачів відчувають себе безпечно в Інтернеті, вважають, що можуть розпізнати сумнівні або нелегітимні сайти (включаючи спроби мімікрії) та перевіряти інформацію за допомогою пошукових інструментів. Регулярно проводяться опитування для оцінки довіри та відчуття захищеності користувачів в Інтернеті.	Майже всі користувачі впевнені, що вони можуть безпечно користуватися Інтернетом для різних цілей і можуть допомогти іншим безпечно користуватися ним. Майже всі користувачі Інтернету відчувають себе захищеними при використанні Інтернету та пошуку достовірного контенту. Опитування мають високу репутацію в регіоні та світі і впливають на розвиток показників в інших країнах.

Фактор - D 2.2: Рівень довіри та впевненості в онлайн-послугах

Аспект	Початковий	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Дезінформація	Провайдери не вирішують питання дезінформації, зокрема, таких як недостовірна інформація, в країні. Цивільному суспільству та іншим недержавним суб'єктам бракує інструментів та ресурсів для протидії дезінформації в Інтернеті, таких як викриття дезінформаційних кампаній. Державні органи та суб'єкти не протидіють дезінформації в Інтернеті.	Провайдери розробляють підходи для вирішення проблем дезінформації в країні. Провідні представники суспільства та недержавних суб'єктів розпочали розробку інструментів та ресурсів для боротьби з дезінформацією. Державні програми та ініціативи щодо боротьби з дезінформацією розробляються, але вони передбачають фільтрацію та обмежені зусилля з інформування користувачів Інтернету.	Провайдери мають ряд підходів до боротьби з дезінформацією; вони поважають свободу вираження поглядів та інших прав людини в Інтернеті. Зацікавлені сторони громадськості розробили інструменти та ресурси для протидії дезінформації в Інтернеті. Державні програми та ініціативи, спрямовані на посилення готовності громадськості до протидії дезінформації в Інтернеті обмежуються підвищенням обізнаності, уникаючи при цьому цензури чи фільтрації інформації.	Провайдери запровадили політику та практику протидії дезінформації; вони поважають свободу вираження поглядів та інші права людини в Інтернеті. Існують спільні зусилля зацікавлених сторін громадськості, які регулярно використовуються для боротьби з дезінформацією в Інтернеті з дотриманням свободи вираження поглядів та інших прав людини в Інтернеті. Опитування, орієнтовані на результат, використовуються для вдосконалення програм та ініціатив, спрямованих на розширення прав і можливостей користувачів та формування розуміння громадськості щодо можливої дезінформації в Інтернеті.	Інтернет-провайдери запровадили політику та практику боротьби з дезінформацією в інноваційні способи, які поважають свободу вираження поглядів та інші права людини в Інтернеті. Спільні зусилля зацікавлених сторін громадськості активно переглядаються з метою врахування більш масштабних стратегічних змін, пов'язаних з дезінформацією та підвищенням рівня обізнаності. Країна підтримує розробку національних/регіональних/міжнародних планів дій та керівних принципів для боротьби з дезінформацією таким чином, щоб захистити Інтернет та розширити права і можливості користувачів.
Довіра користувачів до Державних електронних послуг	Держава пропонує дуже обмежену кількість електронних послуг, якщо такі взагалі існують, і не сприяє публічному забезпеченню Їхньої безпеки. Загалом, суспільство не користується будь-якими серйозними послугами електронного урядування. Не існує опитувань або показників, які б показували, наскільки користувачі Інтернету довіряють послугам електронного урядування. Бракує інформації про безпеку системи електронного урядування.	Влада почала створювати основний набір електронних послуг, для яких вона визнає необхідність застосування заходів безпеки з метою встановлення довіри до їх використання. Обмежена кількість первинних користувачів довіряє безпечному використанню послуг електронного урядування. Показники для оцінки довіри користувачів до послуг електронного урядування обмежені або несистематичні. Державні органи влади готують інформацію про ініціативи та порушення у сфері конфіденційності та безпеки в індивідуальному порядку.	Розроблено ключові сервіси електронного урядування, які залучили значну кількість користувачів. Чимала та зростаюча кількість користувачів Інтернету довіряє використанню послуг електронного урядування. Існують та належним чином фінансуються опитування та показники для оцінки довіри користувачів до послуг електронного урядування. Органи державної влади публікують інформацію та оновлення про виявлені ними порушення конфіденційності та безпеки, а також ініціативи, такі як конфіденційність за замовчуванням.	Послуги електронного урядування стали основним (за замовчуванням) способом надання державних інформаційних послуг. Більшість інтернет-користувачів в країні довіряють безпечності використання сервісів електронного урядування та користуються ними. Регулярно проводяться опитування для оцінки довіри користувачів до послуг електронного урядування. Органи державної влади координують, публікують та інформують користувачів про ініціативи та порушення у сфері конфіденційності та захищеності.	Послуги електронного урядування в країні визнані на регіональному та міжнародному рівнях. Інтернет-користувачі довіряють тому, що послуги електронного урядування постійно перевіряються, вдосконалюються та розширюються з метою підвищення їхньої безпеки. Опитування, орієнтовані на результат, використовуються для аналізу послуг електронного урядування та оцінки управління контентом. Країна є лідером в інформуванні користувачів про поточні та майбутні загрози конфіденційності та захищеності, ініціативи та інші питання.

Фактор - D 2.2: Рівень довіри та впевненості в онлайн-послугах

Аспект	Початковий	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Довіра користувачів до онлайн-послуг	Послуги електронної комерції не надаються. Інтернет-користувачам бракує довіри для користування будь-якими доступними онлайн-послугами. Не існує опитувань або показників, які б показували, наскільки користувачі Інтернету довіряють послугам електронної комерції. Потреба в ініціативах щодо забезпечення безпеки онлайн-послуг майже не визнається або взагалі не усвідомлюється.	Послуги електронної комерції надаються в обмеженому обсязі. Обмежена кількість перших користувачів довіряє безпечному використанню послуг електронної комерції. Показники для оцінки довіри користувачів до послуг електронної комерції обмежені або несистематичні. Приватний сектор визнає необхідність застосування заходів безпеки для встановлення довіри до послуг електронної комерції.	Онлайн-послуги повністю створені різними зацікавленими сторонами в безпечному середовищі. Значна кількість інтернет-користувачів довіряє безпечному використанню послуг електронної комерції. Опитування та показники для оцінки довіри користувачів до послуг електронної комерції запроваджені та належним чином фінансуються. Надійні рішення з безпеки є сучасними та доступними, зокрема, для платіжних систем. Впроваджено схеми сертифікації та довірчі знаки для послуг електронної комерції.	Послуги електронної комерції отримали загальне визнання як безпечна практика для споживачів. Більшість користувачів довіряють безпечному використанню послуг електронної комерції та користуються ними. Регулярно проводяться опитування для оцінки довіри користувачів до онлайн-послуг. Зацікавлені сторони інвестують у розширення функціоналу онлайн-послуг, захист персональної даних та забезпечення зворотного зв'язку з споживачами.	Послуги електронної комерції в країні визнані на регіональному та міжнародному рівнях. Інтернет-користувачі вірять, що послуги електронної комерції активно перевіряються, покращуються та розширюються з метою підвищення їх безпеки. Опитування, орієнтовані на результат, використовуються для аналізу та вдосконалення послуг електронної комерції з метою просування прозорих, надійних та безпечних систем. Правила та умови надання послуг електронної комерції є чіткими та зрозумілими для всіх користувачів.

Фактор - D 2.3: Розуміння користувачем питань захисту персональних даних в Інтернеті

Аспект	Початковий	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Захист персональних даних в Інтернеті	Користувачі та зацікавлені сторони в державному та приватному секторах не мають жодних або мінімальних знань про те, як обробляються персональні дані в Інтернеті, а також не вірять, що існують адекватні заходи для захисту їхніх персональних даних. Дискусія щодо захисту персональних даних в Інтернеті відсутня або обмежена. Не має стандартів конфіденційності, які б визначали правила користування Інтернетом та соціальними мережами.	Користувачі та зацікавлені сторони в державному та приватному секторах можуть мати загальні знання про те, як обробляються персональні дані в Інтернеті; і можуть застосовувати ефективні (проактивні) практики кібербезпеки для захисту своїх персональних даних в Інтернеті. Розпочалися дискусії щодо захисту персональних даних та балансу між безпекою та приватним життям. Розробляються конкретні заходи або політики конфіденційності.	Зростаюча кількість користувачів має навички управління своїм приватним життям в Інтернеті та захисту від вторгнення, втручання або небажаного доступу до інформації з боку інших осіб. Ведеться серйозна публічна дискусія щодо захисту персональних даних та балансу між безпекою та приватним життям. Була розроблена політика конфіденційності в державному та приватному секторах.	Всі зацікавлені сторони мають інформацію, впевненість і можливість вживати заходів для захисту своїх персональних даних в Інтернеті та зберігати контроль над розповсюдженням цієї інформації. Користувачі та зацікавлені сторони в державному та приватному секторах визнають важливість захисту персональних даних в Інтернеті та знають про свої права на конфіденційність. У приватному та державному секторах існують механізми для формування практики використання Інтернету та соціальних мереж і забезпечення того, щоб конфіденційність та безпека не конкурували.	Користувачі мають знання та навички, необхідні для захисту своїх персональних даних в Інтернеті, адаптуючи свої можливості до змін у середовищі ризиків. Політика в приватному та державному секторах активно переглядається з метою забезпечення того, щоб конфіденційність та безпека не конкурували в змінних умовах, і ґрунтується на відгуках користувачів та публічних дискусіях. Запроваджуються та популяризуються нові механізми, такі як конфіденційність за замовчуванням, як інструменти для забезпечення прозорості.

Фактор - D 2.4: Механізми звітування

Аспект	Початковий	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Механізми звітування	Відсутні офіційні механізми звітності, але їх обговорення могло б розпочатися. Користувачі не використовують соціальні мережі для висловлення занепокоєння щодо будь-яких кіберзагроз та проблем. Відсутня статистика зареєстрованих інцидентів.	Державний та/або приватний сектори забезпечують деякі канали для повідомлення про наслідки від кібератак (такі як онлайн-шахрайство, кібербулінг, насильство над дітьми в Інтернеті, викрадення персональних даних, порушення конфіденційності та безпеки та інші інциденти), але ці канали не є скоординованими та використовуються несистематично. Інтернет-користувачі інколи використовують соціальні мережі для інформування інших користувачів. Розробляється система показників зареєстрованих інцидентів.	Механізми звітування створені, розвиваються та регулярно використовуються. Інтернет-користувачі активно використовують соціальні мережі для інформування інших користувачів. Спостерігаються хороші показники щодо зареєстрованих інцидентів.	Механізми скоординованої звітності активно використовуються та популяризуються в державному та приватному секторах. Інтернет-користувачі постійно використовують соціальні мережі для інформування інших користувачів. Показники наслідків від кібератак були використані для перегляду та просування нових політик і практик.	Були розроблені механізми для координації реагування на інциденти між правоохоронними органами та національними силами реагування на інциденти. Інтернет-користувачі звикли використовувати соціальні мережі для інформування інших користувачів та обміну передовим досвідом. Показники регулярно використовуються для інформування політиків та осіб, які приймають рішення.

Фактор - D 2.5: Медіа та онлайн-платформи

Аспект	Початковий	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Засоби масової інформації та соціальні мережі	Засоби масової інформації рідко, якщо взагалі висвітлюють інформацію про кібербезпеку або повідомляють про такі проблеми, як загрози інформаційної безпеки або кіберзлочинність. У соціальних мережах практично не обговорюються питання кібербезпеки. Будь-яке уявлення про інформаторів є негативним і засноване на кримінальних або інших негативних стереотипах.	Складається враження, що засоби масової інформації висвітлюють питання кібербезпеки вибірково, надаючи обмежену інформацію та висвітлюючи конкретні проблеми, з якими люди стикаються в Інтернеті, такі як захист дітей в Інтернеті або кібер-булінг. Складається враження, що в соціальних мережах мало обговорюються питання кібербезпеки. Існують позитивні приклади випадків, коли інформатори мали позитивний вплив на ситуацію.	Кібербезпека вважається поширеною темою в основних засобах масової інформації, а інформація та звіти з різноманітних питань, включаючи загрози інформаційної безпеки та кіберзлочинність, отримують широке розповсюдження. У соціальних мережах ведеться жвава дискусія щодо кібербезпеки. Існує розуміння того, що інформатори можуть відігравати позитивну роль.	Вважається, що засоби масової інформації висвітлюють не лише повідомлення про загрози, але й можуть інформувати громадськість про проактивні та дієві заходи з кібербезпеки, а також про економічні та соціальні наслідки. У соціальних мережах часто обговорюються питання кібербезпеки, і люди постійно використовують соціальні мережі для обміну досвідом. Прозорість заохочується, так само як і інформатори.	Вважається, що обговорення особистого досвіду та особистих поглядів людей в ЗМІ та соціальних мережах є основою для формування політики та сприяють суспільним змінам. Соціальні мережі стали головним інструментом у відстеженні та усуненні загрози інформаційної безпеки. Інформатори заохочуються та захищаються як засіб соціальної відповідальності.

Параметр 3: Формування знань та можливостей у сфері кібербезпеки

У цьому параметрі розглядається наявність, якість і засвоєння програм для різних груп зацікавлених сторін, включаючи державні органи, приватний сектор і населення в цілому, які стосуються програм підвищення обізнаності з питань кібербезпеки, освітніх програм з кібербезпеки, а також програм професійної підготовки.

Фактор
D 3.1: Підвищення обізнаності з питань кібербезпеки

Цей фактор фокусується на доступності програм, які підвищують обізнаність з питань кібербезпеки по всій країні, зосереджуючи увагу на ризиках та загрозах кібербезпеки та методах їх протидії.
> Фактор

Аспекти

- **Державні ініціативи з підвищення обізнаності:** у цьому Аспекті досліджується наявність національної скоординованої програми підвищення обізнаності з питань кібербезпеки, керованої державою, яка охоплює широкий спектр демографічних питань та проблем, розроблених у консультаціях із зацікавленими сторонами з різних галузей.
- **Ініціативи приватного сектору щодо підвищення обізнаності:** у цьому Аспекті розглядається наявність програм підвищення обізнаності, що реалізуються приватним сектором, а також ступінь їх узгодженості з державними ініціативами та ініціативами цивільного суспільства;
- **Ініціативи цивільного суспільства щодо підвищення обізнаності:** цей аспект вивчає наявність програм підвищення обізнаності, що реалізуються цивільним суспільством, а також ступінь їх узгодженості з державними ініціативами та ініціативами приватного сектору; а також
- **Підвищення рівня обізнаності керівників:** цей аспект розглядає зусилля, спрямовані на підвищення рівня обізнаності керівників з питань кібербезпеки в державному, приватному, академічному секторах та секторі цивільного суспільства, а також шляхи подолання ризиків у сфері кібербезпеки.

Фактор
D 3.2: Освіта у сфері кібербезпеки

Цей фактор стосується наявності та забезпечення якісних освітніх програм з кібербезпеки та достатньої кількості кваліфікованих вчителів і викладачів. Крім того, цей фактор розглядає необхідність посилення освіти з кібербезпеки на національному та інституційному рівнях, а також співпрацю між державою та промисловістю для забезпечення того, щоб інвестиції в освіту відповідали потребам освітнього середовища з кібербезпеки в усіх сферах.
> Фактор

Аспекти

- **Забезпечення:** цей Аспект досліджує, чи існують освітні пропозиції з кібербезпеки та кваліфікаційні програми для викладачів, що дають розуміння поточних ризиків та вимог до навичок; та
- **Управління:** цей аспект досліджує координацію та ресурси для розвитку та вдосконалення системи освіти з питань кібербезпеки з виділенням бюджету та витрат на основі національної потреби.

Фактор
D 3.3: Cybersecurity Professional Training

Цей фактор розглядає та аналізує наявність та надання доступних професійних навчальних програм з кібербезпеки з метою формування кадрового потенціалу фахівців з кібербезпеки. Крім того, цей Фактор аналізує рівень засвоєння навчання з кібербезпеки, горизонтальну та вертикальну передачу знань та навичок з кібербезпеки в організаціях, а також те, як ця передача навичок перетворюється на безперервне збільшення фахівців у сфері кібербезпеки.

> Фактор

Аспекти

- **Забезпечення:** у цьому Аспекті розглядається розробка, наявність та надання навчальних програм з кібербезпеки для підвищення кваліфікації та можливостей; а також
- **Опанування:** у цьому Аспекті розглядається розуміння та доступність таких програм для підготовки сертифікованих фахівців з кібербезпеки. Досліджувалися такі питання, як ініціативи щодо реєстрації на такі програми, ініціативи щодо перебування в країні після успішного завершення, обмін знаннями після завершення програми, а також існування національного реєстру успішних та сертифікованих студентів.

Фактор
D 3.4: Дослідження та інновації в галузі кібербезпеки

Цей фактор стосується акценту на дослідженнях та інноваціях у сфері кібербезпеки для вирішення технологічних, суспільних та бізнес-викликів, а також для сприяння підвищенню рівня знань та спроможностей у сфері кібербезпеки в країні.

> Фактор

Аспекти

- **Дослідження та розробки у сфері кібербезпеки:** цей аспект досліджує наявність культури досліджень та інновацій в країні, яка пов'язана з національним переліком поточних та завершених проєктів, фінансовою підтримкою, стимулами та корисними результатами досліджень.

Фактор - D 3.1: Підвищення обізнаності з питань кібербезпеки

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Державні ініціативи	Держава не розробила загальної національної програми підвищення обізнаності з питань кібербезпеки. Потреба в обізнаності щодо загроз та вразливостей кібербезпеки в державних органах не визнається або перебуває лише на початкових стадіях обговорення.	Розробляється скоординована програма підвищення обізнаності з питань кібербезпеки за участю державних органів із залученням відповідних зацікавлених сторін, у тому числі приватного сектору та цивільного суспільства. Ініційовані урядом програми підвищення обізнаності, курси, семінари та онлайн-ресурси доступні, але недостатньо висвітлені в національній стратегії кібербезпеки або перебувають на стадії розробки. Діяльність в рамках програм очолюють різні "виконавці", але вони ще не співпрацюють між собою. Наявність необхідних ресурсів ще не підтверджена. Первинна система механізмів та показників для аналізу процесів обмежена або несистематична.	Опубліковано скоординовану національну програму підвищення обізнаності з питань кібербезпеки з детальним планом її реалізації. Матеріали включають в себе прямі посилання на національну стратегію кібербезпеки. Визначено координаційний орган, наділений достатніми повноваженнями та ресурсами, необхідними для виконання заходів національної програми. Для покращення навичок та знань суспільства існує національний інформаційний портал з питань кібербезпеки, через який поширюється програма. Процеси перегляду програм та показників, націлених на результат, запроваджені, мають належне фінансування та дозволяють оцінювати їхню ефективність.	Національна програма підвищення обізнаності повністю інтегрована з галузевими програмами підвищення обізнаності, орієнтованими на конкретні сфери, наприклад, на промисловість, наукові спільноти, цивільне суспільство та/або жінок і дітей. Регулярно проводиться оцінка нових ризиків у сфері кібербезпеки, що використовується для оновлення національної програми підвищення обізнаності з питань кібербезпеки. Існують підтвердження того, що ці показники використовуються для вдосконалення заходів у рамках національної програми підвищення обізнаності та національної стратегії кібербезпеки.	Національна програма підвищення обізнаності з питань кібербезпеки спільно з зацікавленими сторонами з приватного сектору та цивільного суспільства активно переглядається з метою врахування більш загального стратегічного розвитку в країні (політичного, економічного, соціального, технічного, правового та екологічного). Країна бере активну участь у створенні нових регіональних/ міжнародних програм підвищення обізнаності з питань кібербезпеки, які сприяють розширенню та вдосконаленню міжнародної практики. Національна програма підвищення обізнаності з питань кібербезпеки має відчутний вплив на зменшення загального ландшафту загроз.
Ініціативи приватного сектору	Потреба в обізнаності щодо загроз та вразливостей кібербезпеки в приватному секторі не визнається або перебуває лише на початкових стадіях обговорення.	Існують програми підвищення обізнаності, курси, семінари та онлайнові ресурси, ініційовані приватним сектором, але жодних зусиль з координації та поширення не було зроблено. Первинна система механізмів та показників для аналізу процесів обмежена або несистематична.	Спільні зусилля з підвищення обізнаності (наприклад, спільна політична та/або інформаційно-пропагандистська робота) із зацікавленими сторонами з боку держави та суспільства спрямовані на об'єднання ресурсів, інформації та пошук рішень щодо практик кібербезпеки. Визначено конкретних " виконавців", відповідальних за діяльність в рамках ініціатив приватного сектору, а також створено механізми, що забезпечують координацію між рівнями влади, приватного сектору та суспільства. Існують процеси перегляду програм та показників, націлених на результат, які добре фінансуються та поширюються серед зацікавлених сторін влади та суспільства.	Ефективність спільних зусиль з підвищення обізнаності із зацікавленими сторонами уряду та суспільства регулярно оцінюється та використовується для покращення процесів співробітництва. Ініціативи приватного сектору повністю інтегровані в національну програму підвищення обізнаності. Отримані уроки враховуються при розробці майбутніх програм.	Спільні зусилля з підвищення обізнаності із зацікавленими сторонами уряду та суспільства активно переглядаються з метою врахування більш глобального стратегічного розвитку в країні (політичного, економічного, соціального, технічного, правового та екологічного). Спільні зусилля з підвищення обізнаності із зацікавленими сторонами держави та суспільства мають відчутний вплив на зниження загального рівня загроз.

Фактор - D 3.1: Підвищення обізнаності з питань кібербезпеки

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Ініціативи цивільного суспільства	Потреба в обізнаності щодо загроз та вразливостей кібербезпеки не визнається в суспільстві або перебуває лише на початкових стадіях обговорення.	Є ознаки того, що суспільство усвідомлює, що воно може брати участь у програмах підвищення обізнаності, курсах, семінарах та онлайн-ресурсах, але реальних результатів поки що не видно. Може існувати первинна система показників.	Спільні зусилля з підвищення обізнаності (наприклад, спільна політика та/або інформаційно-роз'яснювальна робота) із зацікавленими сторонами з державного та приватного секторів здійснюються з метою об'єднання ресурсів та інформації, а також пошуку рішень щодо практик кібербезпеки. Функції конкретних "виконавців", які відповідають за дії в рамках ініціатив цивільного суспільства, зрозумілі, і існують механізми, що забезпечують координацію між рівнями влади, приватного сектору та суспільства. Існують процеси перегляду програм та показників, націлених на результат, що добре фінансуються та поширюються серед зацікавлених сторін у державному та приватному секторах.	Ефективність спільних зусиль з підвищення обізнаності з зацікавленими сторонами з державного та приватного секторів регулярно оцінюється та використовується для покращення процесів взаємодії. Ініціативи суспільства повністю інтегровані в національну програму з підвищення обізнаності. Отриманий досвід враховується при розробці майбутніх програм.	Спільні зусилля з підвищення обізнаності з представниками державного та приватного секторів регулярно уточнюються з врахуванням більш загального стратегічного розвитку в країні (політичного, економічного, соціального, технічного, правового та екологічного). Спільні зусилля з підвищення обізнаності з державним та приватним сектором мають значний вплив на зменшення загального ландшафту загроз.
Підвищення рівня обізнаності керівників	Рівень обізнаності керівників з питань кібербезпеки низький або взагалі відсутній. Керівники не усвідомлюють свою відповідальність перед акціонерами, клієнтами, споживачами та працівниками щодо кібербезпеки.	Керівники знають загальні проблеми кібербезпеки, але не знають, як ці проблеми та загрози можуть вплинути на їх організації. Керівники окремих сфер діяльності, таких як фінанси та телекомунікації, були поінформовані про ризики кібербезпеки в цілому, а також про те, як організація вирішує питання кібербезпеки, але не про стратегічні наслідки.	Підвищення обізнаності керівників державного, приватного, наукового секторів та суспільства щодо ризиків кібербезпеки в цілому, основних методів атак, а також того, як організація вирішує проблеми кібербезпеки (як правило, це покладається на CIO*). Обрані керівники інформуються про те, як ризики кібербезпеки впливають на прийняття стратегічних рішень організації, зокрема, у фінансовій та телекомунікаційній сферах. Зусилля з підвищення обізнаності щодо подолання кризових ситуацій у сфері кібербезпеки на рівні виконавчої влади все ще носять рекомендаційний характер.	Зусилля щодо підвищення обізнаності керівників майже в усіх сферах включають визначення стратегічних активів, спеціальних заходів та механізмів, для їх захисту. Керівники можуть змінювати процес прийняття стратегічних рішень і розподіляти конкретні фінансові та людські ресурси на різні елементи кібер-ризику залежно від ситуації, що склалася в компанії. Керівники ознайомлені з планами дій на випадок надзвичайних ситуацій для протидії різним кібератакам та їх наслідкам. Курси підвищення обізнаності керівників з питань кібербезпеки є обов'язковими майже для всіх сфер.	Ризики кібербезпеки розглядаються як питання порядку денного на кожній нараді керівництва, а фінансування та увага спрямовуються на подолання цих ризиків. Керівники на регіональному та міжнародному рівнях розглядаються як джерело передового досвіду у сфері відповідального та підзвітного корпоративного управління кібербезпекою.

* Директор з інформаційних технологій

Фактор - D 3.2: Освіта у сфері кібербезпеки

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Забезпечення	Мало або взагалі немає викладачів з кібербезпеки, а також відсутні кваліфікаційні програми для викладачів. Пропонуються курси з комп'ютерних наук, які можуть мати компонент безпеки, але курси пов'язані з кібербезпекою, не пропонуються. Не існує акредитації у сфері освіти з кібербезпеки.	Вивчається питання щодо кваліфікаційних програм для викладачів з кібербезпеки, зважаючи на невелику кількість наявних кваліфікованих викладачів. Існують деякі освітні курси у сферах, пов'язаних з кібербезпекою, таких як інформаційна безпека, мережева безпека та криптографія, але спеціальні курси з кібербезпеки поки що не пропонуються. Про попит на освіту у сфері кібербезпеки свідчить реєстрація на курси та зворотній зв'язок.	Кваліфікація викладачів у сфері кібербезпеки є легкодоступною. Пропонуються спеціалізовані курси з кібербезпеки, які акредитовані на університетському рівні. Модулі з питань ризиків у сфері кібербезпеки пропонуються як частина багатьох університетських курсів. Університети або еквівалентні навчальні заклади пропонують освіту в сферах, пов'язаних з кібербезпекою. Університети та інші органи проводять семінари/лекції з питань кібербезпеки, орієнтовані на широку аудиторію. Дослідження і розвиток - провідні фактори в освіті з кібербезпеки. Освіта з кібербезпеки не обмежується університетами або еквівалентними навчальними закладами, а охоплює початкову, середню та вищу освіту, а також післядипломну освіту, включаючи професійно-технічну освіту. Можливо, були зроблені кроки для включення STEM* або еквівалентної освітньої програми з акцентом на кібербезпеку в навчальні програми початкової та середньої школи.	Викладачі з кібербезпеки залучаються не лише з академічного середовища, але й створюються можливості для того, щоб промислові та/або державні експерти також займали ці посади. Акредитовані курси з кібербезпеки включені до всіх освітніх програм з комп'ютерних наук. Спеціально пропонується освіта в галузі кібербезпеки, яка охоплює курси та програми в інших сферах, пов'язаних з кібербезпекою, включаючи технічні та гуманітарні елементи, такі як політичні наслідки та міждисциплінарну освіту. Освітні пропозиції з кібербезпеки є виваженими та зосереджені на розумінні поточних ризиків та вимог до навичок. Зміст курсів з кібербезпеки охоплює теми щодо актуальних загроз у сфері кібербезпеки. Національні або міжнародні засади кібербезпеки та/або навчальні рекомендації беруться до уваги навчальними закладами при розробці курсів з кібербезпеки. Для поєднання знань та практичних навичок пропонуються програми стажування у різних виробничих галузях.	Державні курси, наукові ступені та дослідження знаходяться на передовій освіти у сфері кібербезпеки. Освітні програми з кібербезпеки підтримують баланс між збереженням основних компонентів навчальної програми та гнучких процесів, які реагують на швидкі зміни в середовищі кібербезпеки. Актуальні вимоги кібербезпеки враховуються при коригуванні всіх загальноосвітніх навчальних програм.

* Science, Technology, Engineering, and Mathematics

Фактор - D 3.2: Освіта у сфері кібербезпеки

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Управління	Поки що не розглядається необхідність посилення національної освіти у сфері кібербезпеки. Мережа національних контакт-центрів для державних, регуляторних органів, критичних галузей промисловості та навчальних закладів ще не створена. Дискусія щодо того, як скоординоване управління освітою та дослідженнями у сфері кібербезпеки сприяє розвитку національних знань, ще не розпочалася або тільки розпочинається.	Необхідність покращення освіти з кібербезпеки в школах та університетах або еквівалентних навчальних закладах була визначена провідними державними, промисловими та академічними зацікавленими сторонами. Школи, влада та промисловість співпрацюють на спеціальній основі для забезпечення ресурсів, необхідних для надання освіти з кібербезпеки. Державний бюджет, націлений на освіту у сфері кібербезпеки, ще не сформований. Початкова система механізмів та показників для аналізу попиту та пропозиції на курси з кібербезпеки обмежена або несистематична.	Широкі консультації між владою, приватним сектором, науковцями та представниками суспільства визначають пріоритети освіти у сфері кібербезпеки та відображаються у національній стратегії кібербезпеки. Державний бюджет виділяє кошти на національні дослідження та лабораторії з кібербезпеки в університетах або еквівалентних навчальних закладах. Держава та/або підприємства підтримують конкурси, ініціативи та фінансування для студентів та працівників з метою підвищення привабливості кар'єри у сфері кібербезпеки. Запроваджені та добре фінансуються процеси перегляду програм та показників, націлених на результат, для аналізу попиту та пропозиції на курси з кібербезпеки.	Показники використовуються для покращення заходів в рамках інвестицій в освіту задля створення штату експертів з кібербезпеки в країні в усіх сферах. Управління державним бюджетом та витратами на освіту з питань кібербезпеки ґрунтується на загальнодержавному попиті. Кращі навчальні заклади з питань кібербезпеки обмінюються досвідом з іншими державними та міжнародними партнерами. Держава створила науково-дослідні центри передового досвіду у сфері кібербезпеки.	Завдяки програмам партнерства створюються міжнародні центри передового досвіду з кібербезпеки на чолі з інституціями світового рівня. Співпраця між усіма зацікавленими сторонами у сфері освіти з кібербезпеки є звичною і підтвердженою. Зміст освітніх програм з кібербезпеки відповідає практичним проблемам кібербезпеки та бізнес-викликам і забезпечує механізм вдосконалення навчальних планів з урахуванням змін, що відбуваються в цій сфері.

Фактор - D 3.3: Професійна підготовка з кібербезпеки

Аспект	Початковий	Формуючий	Етап становлення	Стратегічний етап	Динамічний етап
Забезпечення	Навчальних програм з кібербезпеки майже не має або вони відсутні.	Потреба у підготовці фахівців з кібербезпеки була зафіксована на державному рівні. Проводиться навчання IT персоналу з питань кібербезпеки, щоб вони могли реагувати на інциденти в разі їх виникнення, але не існує навчання для спеціалістів у сфері кібербезпеки. Пропонується професійна сертифікація ICT*, з деякими модулями або компонентами безпеки. Навчання та сертифікація з найкращих практик можуть бути доступні через міжнародні інтернет-ресурси (наприклад: CISSP**). Спеціальні навчальні курси, семінари та онлайн-ресурси доступні для фахівців у сфері кібербезпеки через державні або приватні джерела, але їх використання обмежене.	Існують структуровані навчальні програми з кібербезпеки, спрямовані на розвиток навичок для формування штату спеціалістів у сфері кібербезпеки. При розробці професійних навчальних курсів враховуються національні або міжнародні стандарти професійної підготовки у сфері кібербезпеки та кращі світові практики. Професійна сертифікація у сфері безпеки пропонується в усіх галузях країни. Добре зрозумілі потреби суспільства, перелік вимог до підготовки кадрів задокументований. Пропонуються навчальні програми для спеціалістів, які не є фахівцями у сфері кібербезпеки. Можуть бути запроваджені державні ініціативи щодо перебування в країні після успішного завершення навчальних програм з кібербезпеки.	Низка навчальних курсів з кібербезпеки розроблена з урахуванням національних стратегічних потреб і відповідає передовому міжнародному досвіду. Навчальні програми визначають пріоритети національної стратегії кібербезпеки. Навчальні програми пропонуються фахівцям з кібербезпеки і зосереджуються на навичках, необхідних для передачі технічно складних проблем людям, які не є технічними фахівцями, наприклад, керівництву і звичайним працівникам. Показники, націлені на результат, отримані з комплексних даних про попит і пропозицію на фахівців з кібербезпеки, використовуються для інформування про способи, тривалість і методики майбутніх навчальних програм.	Державний і приватний сектори співпрацюють у сфері навчання, постійно змінюються і прагнуть розвивати навички, запозичені з обох секторів. Навчальні пропозиції та освітні програми координуються таким чином, щоб закладений у школах фундамент дозволяв навчальним програмам формувати висококваліфіковану робочу силу. Існують програми та механізми заохочення для утримання кваліфікованої робочої сили в країні.
Опанування	Навчання IT-персоналу, призначеного для реагування на інциденти кібербезпеки, обмежено або взагалі відсутнє. Відсутня передача знань від працівників, які пройшли підготовку з кібербезпеки, ненавченим працівникам.	Показники, які оцінюють участь у спеціальних навчальних курсах, семінарах та сертифікаціях, обмежені за обсягом або мають несистематичний характер. Передача знань від працівників, які пройшли підготовку з кібербезпеки, непідготовленим працівникам як у державному, так і в приватному секторах відбувається на нерегулярній основі.	Існує сформований штат сертифікованих співробітників, які пройшли підготовку з питань кібербезпеки, процесів, планування та аналітики. Може існувати державний реєстр успішних і сертифікованих студентів і фахівців. Налагоджено передачу знань від фахівців, які пройшли підготовку з кібербезпеки, до фахівців, які не пройшли таку підготовку, як у державному, так і в приватному секторах. Ініціативи зі створення робочих місць у сфері кібербезпеки в організаціях заохочують роботодавців навчати персонал для того, щоб стати фахівцями у сфері кібербезпеки. Впроваджено процеси перегляду програм та показників, які дозволяють вимірювати прогрес та оцінювати попит і пропозицію на кваліфікованих працівників у сфері кібербезпеки як у державному, так і в приватному секторах. Ці процеси фінансуються в достатньому обсязі.	Успішність навчання з кібербезпеки враховується при розробці майбутніх навчальних програм. Координація підготовки кадрів у всіх сферах забезпечує задоволення державних потреб у фахівцях.	Фахівці з кібербезпеки не лише виконують державні вимоги, але й консультуються з вітчизняними фахівцями за кордоном з метою обміну досвідом та найкращими практиками.

* Інформаційно-комунікаційні технології

** Certified Information Systems Security Professional Сертифікований професіонал в області безпеки інформаційних систем

Фактор - D 3.4: Дослідження та інновації в галузі кібербезпеки

Аспект	Початковий	Формуючий	Етап становлення	Стратегічний етап	Динамічний етап
Дослідження та інновації	Науково-дослідні та дослідно-конструкторські роботи (НДДКР) у сфері кібербезпеки в країні проводяться в обмеженому обсязі або взагалі відсутні. Відсутній доступ до науково-дослідницької діяльності у сфері кібербезпеки з інших країн.	Певна інтеграція НДДКР у сфері кібербезпеки відбувається всередині країни або з країною-партнером, яка розуміє, як НДДКР у сфері кібербезпеки можуть бути застосовані до місцевих реалій країни. Країна може брати участь у відповідних регіональних/ міжнародних спільнотах співпраці у сфері кібербезпеки. Показники ефективності НДДКР у сфері кібербезпеки обмежені за обсягом або несистематичні.	НДДКР у сфері кібербезпеки були створені та зазначені в національній стратегії кібербезпеки. Розробляється стратегія НДДКР. Визначено ресурси та процеси, необхідні для виконання заходів з НДДКР у сфері кібербезпеки. Фінансування є достатнім для реалізації цих заходів. Здійснюється активна регіональна/ міжнародна співпраця з провідними практиками та розробками. Країна бере активну участь та робить свій внесок у регіональні/міжнародні дослідницькі спільноти, пов'язані з кібербезпекою. Впроваджено показники для вимірювання ефективності НДДКР, які дозволяють вимірювати прогрес та вдосконалювати потенціал країни у сфері НДДКР з питань кібербезпеки	Країна активно формує спільноти за інтересами навколо пріоритетних напрямків НДДКР у сфері кібербезпеки. Стратегія НДДКР розроблена та повністю реалізується. Країна робить значний внесок у НДДКР у сфері кібербезпеки та бере активну участь у розбудові інноваційного потенціалу через міжнародні науково-дослідні консорціуми та інвестиції. Взаємодія між академічними установами та промисловістю підтримує НДДКР і використовується для розробки програм з кібербезпеки, які відповідають потребам промисловості.	Країна є провідним гравцем у дослідженнях та інноваціях у сфері кібербезпеки та формує міжнародні дебати щодо розробки стратегічних планів з НДДКР. Країна дивиться вперед, бачить нові проблеми (пов'язані з новими технологіями або новими типами загроз) і використовує НДДКР для підготовки до майбутньої боротьби із загрозами. Країна робить свій внесок у передовий міжнародний досвід НДДКР у сфері кібербезпеки.

Параметр 4: Нормативно-правова база

Цей параметр досліджує спроможність держави розробляти та впроваджувати національне законодавство, яке прямо чи опосередковано стосується кібербезпеки, з особливим акцентом на питаннях регуляторних вимог до кібербезпеки, законодавства щодо кіберзлочинності та суміжних законодавчих актів. Здатність забезпечити виконання цих законів розглядається через спроможність правоохоронних органів, прокуратури, регуляторних органів та суду. Крім того, у цьому параметрі розглядаються такі питання, як формальні та неформальні механізми співробітництва у боротьбі з кіберзлочинністю.

Фактор
D 4.1: Нормативно-правові акти

Цей фактор охоплює різні законодавчі та нормативні акти, що стосуються кібербезпеки, включаючи законодавчі та нормативні положення, матеріальне та процесуальне законодавство у сфері кіберзлочинності, а також оцінку впливу на права людини.

> Фактор

Аспекти

- **Законодавство про кіберзлочинність:** цей аспект досліджує, чи передбачає чинне законодавство кримінальну відповідальність за різні кіберзлочини в профільному законодавстві або в кримінальному кодексі;
- **Нормативно-правові вимоги щодо кібербезпеки:** у цьому аспекті розглядається наявність нормативно-правової бази з питань кібербезпеки;
- **Процесуальне законодавство щодо кіберзлочинності:** цей аспект досліджує, чи впроваджено комплексне кримінально-процесуальне законодавство - з процесуальними повноваженнями для розслідування кіберзлочинів та вимогами до доказів для протидії, реагування та кримінального переслідування кіберзлочинів та злочинів, пов'язаних з електронними доказами; та
- **Вплив на права людини:** цей аспект досліджує, чи проводиться оцінка впливу на права людини основного та процесуального законодавства про кіберзлочинність та нормативно-правових актів у сфері кібербезпеки.

Фактор
D 4.2: Законодавча база

Цей фактор стосується законодавчої бази, пов'язаної з кібербезпекою, включаючи захист даних, захист дітей, захист прав споживачів та інтелектуальної власності.

> Фактор

Аспекти

- **Захист даних:** у цьому аспекті розглядається наявність та дотримання законодавства про захист даних;
- **Захист дітей в Інтернеті:** цей аспект зосереджений на правовому захисті дітей в Інтернеті, включаючи захист їх прав в Інтернеті та кримінальну відповідальність за жорстоке поводження з дітьми в Інтернеті;
- **Захист прав споживачів:** у цьому аспекті розглядається наявність та дотримання законодавства, що захищає споживачів в Інтернеті від шахрайства та інших форм неправомірних дій у сфері бізнесу; та
- **Законодавство про інтелектуальну власність:** цей аспект стосується існування та дотримання законодавства про інтелектуальну власність в Інтернеті.

Фактор
D 4.3: Правові та регуляторні спроможності

Цей фактор вивчає здатність правоохоронних органів розслідувати кіберзлочини, здатність прокуратури представляти справи про кіберзлочини та електронні докази, а також здатність суду розглядати справи про кіберзлочини та справи, пов'язані з електронними доказами. Нарешті, цей фактор розглядає наявність міжгалузевих регуляторних органів, які здійснюють нагляд за дотриманням конкретних нормативно-правових актів у сфері кібербезпеки.

> Фактор

Аспекти

- **Правоохоронна діяльність:** у цьому аспекті розглядається, чи пройшли співробітники правоохоронних органів та відомств підготовку з питань розслідування та ведення справ про кіберзлочини, а також справ, пов'язаних з електронними доказами, і чи є відповідні людські, процесуальні та технологічні ресурси;
- **Обвинувачення:** у цьому аспекті розглядається, чи пройшли прокурори підготовку з питань розгляду справ про кіберзлочини та справ, пов'язаних з електронними доказами, а також чи є необхідні людські, процесуальні та технологічні ресурси;
- **Суди:** у цьому аспекті розглядається, чи мають суди достатні ресурси та підготовку для забезпечення ефективного та результативного судового переслідування у справах про кіберзлочини та справах, пов'язаних з електронними доказами; а також
- **Регуляторні органи:** у цьому аспекті розглядається існування міжгалузевих регуляторних органів, які здійснюють нагляд за дотриманням конкретних нормативно-правових актів у сфері кібербезпеки.

Фактор
D 4.4:Офіційні та неофіційні механізми співпраці для боротьби з кіберзлочинністю

Цей фактор стосується існування та функціонування офіційних та неофіційних механізмів, які забезпечують співробітництво між внутрішніми та міжнародними суб'єктами з метою стримування та боротьби з кіберзлочинністю.

> Фактор

Аспекти

- **Співпраця правоохоронних органів з приватним сектором:** цей аспект розглядає механізм обміну інформацією про кіберзлочинність між державним та приватним секторами, включаючи співпрацю з Інтернет-провайдерами та іншими постачальниками послуг;
- **Співпраця з іноземними правоохоронними органами:** у цьому аспекті розглядається наявність офіційних механізмів міжнародного співробітництва правоохоронних органів; та
- **Співпраця держави та сектору кримінального правосуддя:** у цьому аспекті розглядаються офіційні канали зв'язку між державою та суб'єктами кримінального правосуддя.

Фактор - D 4.1: Нормативно-правові акти

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Законодавство про кіберзлочинність	Окремого кримінального закону про кіберзлочинність не існує. Можливо, існує основне кримінальне законодавство, але його застосування до кіберзлочинів невизначене.	Існує законодавство, яке частково стосується деяких аспектів кіберзлочинності, або правові положення щодо кіберзлочинності перебувають на стадії розробки.	Основні правові положення щодо кіберзлочинності містяться у спеціальному законодавстві або кримінальному кодексі. Країна може ратифікувати регіональні або міжнародні механізми щодо кіберзлочинності. Країна послідовно прагне запровадити ці механізми у національне законодавство.	Де це доцільно, вживаються заходи для перевищення мінімальних базових показників, визначених міжнародними договорами. Країна прагне адаптувати своє законодавство у сфері боротьби з кіберзлочинністю з урахуванням нових технологій та їх використання.	Законодавство про кіберзлочинність побудовано таким чином, щоб воно могло відповідати динамічним змінам у базових технологіях та загрозах без необхідності суттєвого та тривалого перегляду. Країна активно сприяє просуванню на міжнародному рівні дієвих законодавчих актів у сфері боротьби з кіберзлочинністю.
Нормативно-правові вимоги щодо кібербезпеки	Існують обмежені вимоги щодо кібербезпеки, викладені в нормативно-правових актах. Необхідність створення нормативно-правової бази з питань кібербезпеки, можливо, була визнана і, певно, призвела до проведення аналізу існуючих недоліків.	Були проведені консультації із зацікавленими сторонами з відповідних сфер з метою підтримки створення нормативно-правової бази. Можуть існувати законопроекти та нормативно-правові акти, але вони ще не прийняті і не охоплюють всі необхідні галузі.	Вимоги до кібербезпеки викладені у відповідних нормативно-правових актах (у тому числі в галузевих вимогах, де це доречно). Ці вимоги можуть включати обов'язкові стандарти або вимоги щодо повідомлення про порушеня безпеки та виявлення вразливостей. Відповідна цивільна та кримінальна відповідальність чітко сформульована та зрозуміла суб'єктам регулювання. Відповідні законодавчі та регуляторні органи мають повноваження, необхідні для забезпечення виконання цих вимог.	Ефективність законів та нормативно-правових актів щодо покращення практики кібербезпеки регулярно оцінюється та використовується для їх подальшого розвитку. Положення оновлюються з урахуванням новітніх технологій.	Нормативно-правова база є достатньо гнучкою для того, щоб відповідати швидким змінам у технологічному середовищі чи загрозах. На міжнародному рівні країна популяризує найкращі практики правового та регуляторного забезпечення. Країна бере активну участь у розробці міжнародних угод, спрямованих на сприяння гармонізації та взаємному визнанню законів і нормативно-правових актів у сфері кібербезпеки.

Фактор - D 4.1: Нормативно-правові акти

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Процесуальне законодавство щодо кіберзлочинності	Окремого процесуального кримінального законодавства щодо кіберзлочинів не існує. Незрозуміло, як кримінально-процесуальне законодавство застосовується до розслідувань кіберзлочинів, судового переслідування та електронних доказів.	Розпочато розробку спеціального процесуального законодавства щодо кіберзлочинів або внесення змін до загального процесуального кримінального законодавства для адаптації до справ стосовно кіберзлочинів.	Прийнято та застосовується комплексне кримінально-процесуальне законодавство, що містить положення про розслідування кіберзлочинів та вимоги до доказів. Країна може ратифікувати регіональні або міжнародні документи щодо кіберзлочинності. Країна прагне послідовно запровадити ці положення у своє законодавство. Процесуальне законодавство, що стосується кіберзлочинності, дозволяє обмін інформацією (та інші необхідні дії) для підтримки успішного міжнародного розслідування кіберзлочинів.	Де це доцільно, вживаються заходи для перевищення мінімальних базових показників, визначених міжнародними договорами. Країна прагне адаптувати процесуальне законодавство щодо кіберзлочинності з урахуванням нових технологій та їх використання.	Процесуальне законодавство у сфері кіберзлочинності побудовано таким чином, щоб воно могло відповідати динамічним змінам у технологіях та загрозах, без необхідності тривалого перегляду. Країна активно сприяє просуванню дієвого процесуального законодавства у сфері кіберзлочинності та інструментів, що покращують міжнародні розслідування кіберзлочинів.
Вплив на права людини	Законодавство про кіберзлочинність та положення про кібербезпеку можуть перебувати на стадії розробки, але жодного оцінювання їх впливу на права людини не проводилося.	Можливо, було проведено оцінку впливу на права людини законодавства про кіберзлочинність та нормативно-правових актів у сфері кібербезпеки, включаючи розгляд наслідків для приватного життя та свободи вираження поглядів. Однак, деякі питання ще не вирішені. При розробці законодавства та нормативно-правових актів були проведені консультації з експертами з прав людини.	Завершено оцінювання впливу на права людини основного та процесуального законодавства про кіберзлочинність та нормативно-правових актів з питань кібербезпеки, які відповідають міжнародним стандартам. Реалізація цього законодавства регулярно перевіряється на предмет дотримання прав людини, і це незалежна перевірка.	Оцінки впливу на права людини регулярно переглядаються для забезпечення того, щоб практика залишалася сумісною з вимогами прав людини, а також для врахування впливу нових технологій. Було також розглянуто питання про те, як кібербезпека може посилити захист прав людини в країні та на міжнародному рівні.	Країна активно сприяє розвитку та просуванню процедури оцінки впливу на права людини стосовно кібербезпеки.

Фактор - D 4.2: Законодавча база

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Захист даних	Законодавства про захист даних не існує.	Розробляється законодавство про захист персональних даних. Були проведені консультації із зацікавленими сторонами з відповідних сфер з метою підтримки розробки цього законодавства.	Прийнято та впроваджено законодавство про захист персональних даних, яке відповідає міжнародним стандартам та найкращим практикам. Визначено головний орган, відповідальний за забезпечення захисту даних.	Ефективність законодавства у сфері захисту персональних даних регулярно оцінюється та враховується при його доопрацюванні. Країна прагне адаптувати законодавство про захист даних з урахуванням нових технологій та їх використання.	Законодавство про захист даних побудовано таким чином, щоб враховувати зміни, що відбуваються в технологічному середовищі та характері загроз, без необхідності його суттєвого доопрацювання. Країна розвиває та впроваджує міжнародні стандарти регулювання законодавства у сфері захисту персональних даних. Країна бере активну участь у розробці правових механізмів, що сприятимуть покращенню міжнародного співробітництва у цій сфері.
Захист дітей в Інтернеті	Законодавство, щодо захисту дітей, обмежене, і його застосування в онлайн середовищі ще не розглядалося.	Існує законодавство щодо захисту дітей, яке адаптується з врахуванням його застосування в інтернет-середовищі. З метою підтримки розробки та адаптації цього законодавства були проведені консультації із зацікавленими сторонами з відповідних галузей.	Питання захисту дітей в онлайн-середовищі знайшло розуміння та відображення у відповідному законодавстві. Законодавство впроваджується відповідно до міжнародних стандартів та найкращих практик.	Ефективність законодавства про захист дітей в Інтернеті регулярно оцінюється та враховується при його доопрацюванні. Країна прагне адаптувати законодавство про захист дітей з урахуванням нових технологій та їх використання.	Законодавство про захист дітей в Інтернеті побудовано таким чином, щоб воно могло враховувати динамічні зміни в технологіях та характері загроз, без необхідності суттєвого коригування. Країна розробляє та впроваджує міжнародні стандарти законодавства щодо захисту дітей в Інтернеті. Країна бере активну участь у розробці правових механізмів, що сприятимуть покращенню міжнародного співробітництва у цій сфері.

Фактор - D 4.2: Законодавча база

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Захист прав споживачів	Законодавство, пов'язане із захистом прав споживачів, обмежене, і його застосування в онлайн-середовищі ще не розглядалося.	Існує законодавство про захист прав споживачів, яке адаптується з урахуванням його застосування в онлайн-середовищі. З метою підтримки розробки цього законодавства були проведені консультації із зацікавленими сторонами з відповідних галузей.	Питання захисту прав споживачів в онлайн-середовищі знайшло розуміння та висвітлення у відповідному законодавстві. Законодавство впроваджується відповідно до міжнародних стандартів та найкращих практик.	Ефективність законодавства про захист прав споживачів в Інтернеті регулярно оцінюється та враховується при його доопрацюванні. Країна прагне адаптувати законодавство про захист прав споживачів з урахуванням нових технологій та їх використання.	Законодавство про захист прав споживачів побудовано таким чином, щоб воно могло відповідати динамічним змінам у технологіях та характері загроз без необхідності суттєвого коригування. Країна розробляє та впроваджує міжнародні стандарти у сфері захисту прав споживачів в Інтернеті. Країна бере активну участь у розробці правових механізмів, що сприятимуть покращенню міжнародного співробітництва у цій сфері.
Законодавство про інтелектуальну власність	Законодавство, щодо захисту інтелектуальної власності, обмежене, а його застосування в онлайн середовищі ще не розглядалося.	Існує законодавство, щодо захисту інтелектуальної власності, яке адаптується з урахуванням його застосування в онлайн-середовищі. З метою підтримки розробки цього законодавства були проведені консультації із зацікавленими сторонами з відповідних галузей.	Питання захисту інтелектуальної власності в онлайн-середовищі знайшло розуміння та відображення у відповідному законодавстві. Законодавство впроваджується відповідно до міжнародних стандартів та найкращих практик.	Ефективність законодавства про захист інтелектуальної власності в Інтернеті регулярно оцінюється та враховується при його доопрацюванні. Країна прагне адаптувати законодавство про захист інтелектуальної власності з урахуванням нових технологій та їх використання.	Законодавство про інтелектуальну власність побудовано таким чином, щоб воно могло відповідати динамічним змінам у технологіях та характері загроз без необхідності суттєвого коригування. Країна розробляє та впроваджує міжнародні стандарти щодо захисту прав інтелектуальної власності в Інтернеті. Країна бере активну участь у розробці правових механізмів, що сприятимуть покращенню міжнародного співробітництва у цій сфері.

Фактор - D 4.3: Правові та регуляторні спроможності

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Правоохоронна діяльність	Правоохоронці не мають достатніх спроможностей для запобігання та боротьби з кіберзлочинністю та не проходять спеціальної підготовки з розслідування кіберзлочинів.	До розслідувань кіберзлочинів застосовуються традиційні слідчі заходи, але можливості цифрової криміналістики обмежені. Правоохоронці можуть проходити навчання з питань кіберзлочинності та збору цифрових доказів, але це відбувається нерегулярно.	Створено комплексну інституційну спроможність з достатніми людськими, процесуальними та технологічними ресурсами для розслідування кіберзлочинів. Створено систему зберігання цифрових даних та забезпечення цілісності доказів, включаючи формальні процеси, ролі та обов'язки. Існують та впроваджуються стандарти підготовки працівників правоохоронних органів з питань кіберзлочинності та збору цифрових доказів. Національні та державні/місцеві правоохоронні органи розуміють власні функції, та оснащені для їх виконання.	Кількісна оцінка ризиків використовується для розподілу ресурсів між оперативними підрозділами по боротьбі з кіберзлочинністю (на державному та регіональному рівнях). Тенденції та статистика щодо кіберзлочинності, втручання правоохоронних органів та їх впливу на зменшення шкоди збираються, аналізуються та використовуються для формування стратегії та прийняття рішень щодо розподілу ресурсів на довгострокову перспективу. Правоохоронні стратегії включають заходи з попередження злочинності поряд з правоохоронними заходами. Розвідувальні дані використовуються для підтримки проактивних розслідувань. Правоохоронні органи мають можливості підтримувати цілісність даних, щоб відповідати міжнародним стандартам доказової бази при проведенні міжнародних розслідувань.	Країна бере активну участь у розвитку платформ співпраці між національними правоохоронними органами. Правоохоронні органи країни знаходяться в епіцентрі розробки нових інструментів та підходів для запобігання та протидії кіберзлочинності, а також сприяння їх використанню на міжнародному рівні.
Обвинувачення	Прокурори не мають належної підготовки та ресурсів для аналізу електронних доказів або притягнення до відповідальності за кіберзлочини. Можливо, розпочалися консультації щодо розгляду цієї можливості в прокурорській спільноті.	Обмежена кількість прокурорів має компетенцію щодо ведення справ про кіберзлочини та роботи з електронними доказами, але ця діяльність є епізодичною та не є офіційно закріпленою. Прокурори проходять навчання з питань кіберзлочинності та цифрових доказів, але це відбувається епізодично.	Створено комплексну інституційну спроможність, включаючи достатні людські та технологічні ресурси, для судового переслідування у справах про кіберзлочини та справах, пов'язаних з електронними доказами. Можливо, буде створено штат кваліфікованих прокурорів з питань кіберзлочинності.	Створено інституційні структури з чітким розподілом завдань та обов'язків в органах прокуратури на всіх рівнях держави. Існує механізм, який дозволяє обмінюватися інформацією та передовим досвідом між прокурорами та суддями для забезпечення ефективного та результативного кримінального провадження у справах про кіберзлочини.	Існує національна спроможність здійснювати судове переслідування складних внутрішніх та міжнародних кіберзлочинів.

Фактор - D 4.3: Правові та регуляторні спроможності

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Суди	Немає процесу підготовки суддів для того, щоб вони могли розглядати справи про кіберзлочини або справи, пов'язані з електронними доказами. Можливо, почалися консультації щодо розгляду цієї можливості в суддівській спільноті.	Обмежена кількість суддів має можливість розглядати справи щодо кіберзлочинів, але ця можливість є нерегулярною. Якщо судді проходять підготовку з питань кіберзлочинності та цифрових доказів, то вона носить епізодичний характер.	Наявні достатні людські та технологічні ресурси для забезпечення ефективного та результативного судочинства у справах про кіберзлочини та справах, пов'язаних з електронними доказами. Судді проходять спеціальну підготовку з питань кіберзлочинності та електронних доказів. Державні/місцеві суди забезпечені обладнанням для розгляду справ про кіберзлочини відповідно до їх рівня. Відповідні суди спроможні розглядати цивільні позови, пов'язані з відповідальністю за порушення кібербезпеки.	Інституційна спроможність судової системи розглядати справи про кіберзлочини часто аналізується та переглядається на основі оцінки ефективності.	Країна бере активну участь у розробці та поширенні найкращих практик ведення справ щодо кіберзлочинів.
Регуляторні органи	Галузеві регуляторні органи мають обмежене розуміння потенційного впливу кіберзлочинності на їх суб'єкти регулювання. Не існує міжгалузевого регуляторного органу, який би здійснював нагляд за дотриманням певних вимог у сфері кібербезпеки.	Галузеві регуляторні органи почали визначати свої функції у сфері кібербезпеки. Можна було розглянути питання про створення міжгалузевих регуляторних органів для нагляду за дотриманням певних нормативно-правових актів у сфері кібербезпеки. В ході цього процесу були проведені консультації з відповідними зацікавленими сторонами.	Галузеві регуляторні органи (наприклад, фінанси, енергетика, транспорт) забезпечені можливостями та ресурсами, необхідними для здійснення нагляду за дотриманням вимог кібербезпеки у своїй галузі. Там, де створені міжгалузеві регуляторні органи для нагляду за кібербезпекою, вони мають необхідні можливості та ресурси для виконання своїх функцій.	Вплив регуляторних заходів на практику організацій у сфері кібербезпеки регулярно оцінюється та використовується для інформування органів нагляду та розробки нормативно-правових актів. Регуляторні органи постійно оцінюють новітні технології та їх потенційний вплив на кібербезпеку суб'єктів регулювання. Регуляторне втручання та розслідування базуються на національній оцінці кібер-ризиків та визначають пріоритети на основі цих оцінок.	Регуляторні органи беруть активну участь у розробці та поширенні передового досвіду регулювання на міжнародному рівні.

Фактор - D 4.4:Офіційні та неофіційні механізми співпраці для боротьби з кіберзлочинністю

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Співпраця правоохоронних органів з приватним сектором	Співпраця між державним та приватним секторами у сфері боротьби з кіберзлочинністю обмежена. Зокрема, не налагоджена співпраця між Інтернет-провайдерами та іншими постачальниками технологічних послуг і правоохоронними органами.	Обмін інформацією про кіберзлочинність між державним та приватним секторами є нерегулярним та нерегламентованим. Співпраця між Інтернет-провайдерами та іншими постачальниками технологічних послуг і правоохоронними органами існує, але не завжди ефективна.	Обмін інформацією між державним та приватним секторами здійснюється на регулярній основі та підкріплюється відповідним законодавством. В рамках співпраці між державним та приватним секторами були створені ефективні механізми співпраці між Інтернет-провайдерами та іншими постачальниками технологічних послуг, а також правоохоронними органами.	Ефективність співпраці між державним та приватним секторами регулярно оцінюється та використовується для покращення співпраці. Механізми співробітництва регулярно адаптуються з урахуванням нових технологій та нових форм кіберзлочинності.	Країна активно сприяє розвитку державно-приватного партнерства та розбудові міжнародних платформ державно-приватного партнерства.
Співпраця з іноземними правоохорон-ними органами	Форми міжнародного співробітництва у сфері запобігання та протидії кіберзлочинності мінімальні або взагалі відсутні.	Офіційні механізми міжнародного співробітництва правоохоронних органів існують, але вони не застосовуються до кіберзлочинності або застосовуються лише в окремих випадках. Правоохоронні органи офіційно не включені в регіональні та міжнародні мережі з боротьби з кіберзлочинністю.	Створено офіційні механізми міжнародного співробітництва правоохоронних органів з метою сприяння виявленню, розслідуванню та кримінальному переслідуванню кіберзлочинів. Створені та застосовуються угоди та механізми взаємної правової допомоги, екстрадиції у справах, пов'язаних з кіберзлочинністю. Правоохоронні органи країни інтегровані з регіональними та міжнародними структурами, такими як Інтерпол або система 24/7.	Правоохоронні органи працюють спільно з іноземними партнерами, в рамках спільних оперативних груп, що призводить до успішних міжнародних розслідувань кіберзлочинів та судових переслідувань.	Країна активно сприяє просуванню та розвитку механізмів міжнародного співробітництва.
Співпраця держави та сектору кримінального правосуддя	Існує мінімальна взаємодія між державними органами та суб'єктами кримінального судочинства.	Обмін інформацією між державними органами та суб'єктами кримінального судочинства обмежений і носить епізодичний характер.	Встановлено офіційні відносини між державними органами та суб'єктами кримінального судочинства, що призвело до постійного обміну інформацією з питань кіберзлочинності.	Взаємовідносини між державними суб'єктами, прокурорами, суддями та правоохоронними органами регулярно оцінюються та застосовуються для підвищення їх ефективності.	Країна активно долучається до міжнародного просування ефективного та своєчасного обміну інформацією між державними органами та суб'єктами кримінального судочинства.

Параметр 5: Стандарти та технології

Цей Параметр розглядає ефективне та широке використання технологій кібербезпеки для захисту окремих осіб, організацій та національної інфраструктури. Зокрема, у рамках цього напрямку розглядається впровадження стандартів і передового досвіду у сфері кібербезпеки, розгортання процесів і засобів контролю, а також розвиток технологій і продуктів з метою зменшення ризиків у сфері кібербезпеки.

Фактор
D 5.1: Дотримання стандартів

Цей фактор оцінює спроможність держави просувати, оцінювати впровадження та контролювати дотримання міжнародних стандартів і передового досвіду у сфері кібербезпеки.

> Фактор

Аспекти

- **Стандарти безпеки ІКС:** цей аспект досліджує, чи застосовуються та впроваджуються в державному секторі та організаціях КІ стандарти та передові практики, пов'язані з кібербезпекою;
- **Стандарти закупівель:** цей аспект стосується впровадження стандартів та передового досвіду в усіх галузях для управління процесами закупівель, включаючи управління ризиками, управління життєвим циклом, забезпечення якості програмного та апаратного забезпечення, аутсорсинг та використання хмарних сервісів; а також
- **Стандарти постачання товарів та послуг:** цей аспект стосується використання стандартів та передових практик місцевими постачальниками товарів та послуг, включаючи програмне забезпечення, апаратне забезпечення, керовані послуги та хмарні сервіси.

Фактор
D 5.2: Засоби контролю безпеки

Цей фактор перевіряє інформацію щодо розгортання засобів контролю безпеки користувачами, державним і приватним секторами, а також щодо того, чи базується набір засобів контролю технологічної кібербезпеки на встановлених засадах кібербезпеки.

> Фактор

Аспекти

- **Технологічні заходи контролю безпеки:** цей аспект досліджує, якою мірою сучасні заходи контролю технологічної безпеки, включаючи патчі та резервні копії, впроваджені в усіх галузях; а також
- **Криптографічний контроль:** у цьому Аспекті розглядається застосування криптографічних методів всіма галузями та користувачами для захисту даних, що зберігаються або передаються, а також те, наскільки цей криптографічний контроль відповідає міжнародним стандартам і керівним принципам та підтримується в актуальному стані.

Фактор
D 5.3: Якість програмного забезпечення

Цей фактор досліджує якість розгортання програмного забезпечення, а також вимоги до його функціональності в державному та приватному секторах.
Крім того, цей Фактор перевіряє існування та вдосконалення політик і процесів для оновлення, а також обслуговування програмного забезпечення на основі оцінки ризиків і критичного характеру послуг.

> Фактор

Аспекти

- **Гарантія якості програмного забезпечення:** (як зазначено вище)

Фактор
D 5.4: Стійкість інфраструктури зв 'язку та Інтернету

Цей фактор стосується наявності надійних Інтернет-послуг та інфраструктури в країні, а також суворих заходів безпеки в приватному та державному секторах. Крім того, цей фактор розглядає контроль, який держава може мати над Інтернет інфраструктурою, та ступінь, в якому мережі та системи передаються на аутсорсинг.

> Фактор

Аспекти

- **Надійність Інтернет-інфраструктури:** цей аспект вивчає надійність та захист Інтернет-послуг та інфраструктури в державному та приватному секторах; та
- **Моніторинг та реагування:** у цьому Аспекті розглядається, чи існують механізми для проведення оцінки ризиків та моніторингу стійкості мережі як у державному, так і в приватному секторах.

Фактор
D 5.5: Ринок кібербезпеки

Цей фактор розглядає наявність та розвиток конкурентоспроможних технологій кібербезпеки, продуктів кібер-страхування, послуг та експертизи у сфері кібербезпеки, а також наслідки аутсорсингу для безпеки.

> Фактор

Аспекти

- **Технології кібербезпеки:** у цьому Аспекті розглядається, чи існує і підтримується національний ринок технологій кібербезпеки та чи відповідає він національним потребам;
- **Консультаційні послуги та експертиза з кібербезпеки:** цей аспект досліджує доступність консультаційних послуг з кібербезпеки для приватних та державних організацій;
- **Наслідки аутсорсингу для безпеки:** в цьому Аспекті розглядається, чи проводиться оцінка ризиків для визначення шляхів зменшення ризиків аутсорсингу IT третім особам або хмарним сервісам; та
- **Кібер-страхування:** цей Аспект досліджує існування ринку кібер-страхування, його охоплення та продукти, прийнятні для різних організацій.

Фактор
D 5.6: Відповідальне оприлюднення даних

Цей Фактор досліджує створення механізму належного оприлюднення інформації для отримання та розповсюдження інформації про вразливості в різних сферах, а також наявність достатнього потенціалу для постійного аналізу та оновлення цього механізму.

> Фактор

Аспекти

- **Обмін інформацією про вразливості:** у цьому Аспекті досліджуються існуючі механізми або канали обміну інформацією про технічні деталі вразливостей між зацікавленими сторонами; та
- **Політика, процеси та законодавство щодо належного розкриття недоліків системи безпеки:** цей Аспект досліджує наявність політики або системи належного розкриття інформації в організаціях державного та приватного сектору, а також права на юридичний захист для тих, хто розголошує про недоліки системи безпеки.

Фактор - D 5.1: Дотримання стандартів

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Стандарти безпеки ІКС	Не було визначено жодних стандартів чи передових практик щодо захисту даних, технологій чи інфраструктури в державному та приватному секторах. Або державним та приватним секторами були визначені деякі відповідні стандарти та передові практики, а також, можливо, здійснена певна робота по їх впровадженню, але не було докладено зусиль для впровадження або зміни існуючої практики.	Для використання були визначені стандарти управління інформаційними ризиками, наявні деякі ознаки їх поширення та впровадження в державному та приватному секторах. Наявні певні ознаки впровадження та використання міжнародних стандартів і передового досвіду.	На національному рівні було визначено та впроваджено базові стандарти та найкращі практики у сфері кібербезпеки, які широко застосовуються у державному та приватному секторах. В уряді існує орган, який аналізує використання стандартів у державному та приватному секторах. Існують державні програми для сприяння подальшому розвитку, а також застосовуються метрики для контролю за дотриманням вимог. Розглядається питання про те, як державні органи та КІ можуть використовувати стандарти та найкращі практики для управління ризиками в ланцюгах постачання в межах КІ.	Держава та організації підтримують використання стандартів та найкращих практик відповідно до оцінки національних ризиків та бюджетних рішень. Постійно переглядається перелік стандартів та найкращих практик, а також їх впровадження. Нові ризики кібербезпеки постійно оцінюються та використовуються для переоцінки потреби в додаткових стандартах безпеки ІКС. Існують факти дискусій між державою та іншими зацікавленими сторонами щодо того, як рішення про національні та організаційні ресурси повинні узгоджуватися та сприяти впровадженню стандартів. Докази участі у роботі міжнародних органів зі стандартизації, сприяє розвитку ідейного лідерства та обміну досвідом між організаціями.	Країна бере активну участь у розробці та впровадженні визначених стандартів на міжнародному рівні. Впровадження стандартів та рішення про невідповідність приймаються у відповідь на зміну характеру загроз та ресурсних факторів у всіх галузях КІ шляхом спільного управління ризиками. Існують докази дискусій в усіх галузях щодо дотримання стандартів та найкращих практик, які базуються на постійній оцінці потреб.

Фактор - D 5.1: Дотримання стандартів

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Стандарти закупівель	Не було визначено жодних стандартів або кращих практик для використання в якості керівних принципів при здійсненні закупівель у державному та приватному секторах. Якщо вони і існують, то їх впровадження має несистемний та нескоординований характер	Визначено стандарти та найкращі практики кібербезпеки, що регулюють процеси закупівель (включаючи управління ризиками, управління життєвим циклом, програмне та апаратне забезпечення, аутсорсинг та використання хмарних сервісів), що будуть застосовуватись. У державному та приватному секторах є приклади впровадження стандартів кібербезпеки та найкращих практик у встановленні процедури закупівель.	Стандарти кібербезпеки та передові практики в управлінні процесами закупівель (включаючи управління ризиками, управління життєвим циклом, програмне та апаратне забезпечення, аутсорсинг та використання хмарних сервісів) широко впроваджуються в державному та приватному секторах. Впровадження та дотримання стандартів у практиці закупівель у державному та приватному секторах підтверджується шляхом моніторингу та оцінки ефективності процесів.	Організації мають можливість контролювати та змінювати використання стандартів та найкращих практик у процесах закупівель, за потреби приймати рішення про відхилення та невідповідність на основі оцінки ризиків. Нові ризики кібербезпеки регулярно оцінюються та використовуються для переоцінки потреб у додаткових стандартах у сфері закупівель. Критичні аспекти закупівель та постачання, такі як загальна вартість життєвого циклу, якість, сумісність, технічне обслуговування, підтримка та інші види діяльності, що додають вартість, постійно покращуються, а вдосконалення процесу закупівель здійснюється в контексті загального планування ресурсів. Організації можуть оцінювати навички своїх фахівців із закупівель відповідно до компетенцій, викладених у стандартах закупівель, та виявляти будь-які прогалини у навичках та можливостях.	Країна бере активну участь у розробці та популяризації цих стандартів на міжнародному рівні. Впровадження стандартів у процеси закупівель та прийняття рішень щодо невідповідності стандартам приймаються у відповідь на зміну характеру загроз.
Стандарти постачання товарів та послуг	Для забезпечення захисту продуктів та послуг (зокрема, програмного забезпечення, обладнання, керованих послуг та хмарних сервісів), що розробляються або пропонуються провайдерами в країні, не було визначено стандартів або кращих практик.	У професійних спільнотах визначаються та обговорюються основні заходи та методології безпечної розробки та управління життєвим циклом програмного та апаратного забезпечення, а також надання керованих послуг та хмарних сервісів. Влада популяризує відповідні стандарти у сфері розробки програмного забезпечення, забезпечення якості апаратного забезпечення, надання керованих послуг та безпеки хмарних технологій, але поки немає ознак широкого впровадження цих стандартів.	Існують підтвердження активного впровадження стандартів у процеси розробки програмного забезпечення, забезпечення якості апаратного забезпечення, надання керованих послуг та хмарних сервісів організаціями державного та приватного сектору. Держава має затверджену програму підтримки та моніторингу прийняття стандартів у сфері розробки програмного забезпечення, забезпечення якості апаратного забезпечення та безпеки хмарних технологій для державних та комерційних систем. Високоінтегровані системи та методи розробки програмного забезпечення використовуються в освітніх та навчальних програмах в країні.	Питання безпеки враховуються на всіх етапах розробки програмного та апаратного забезпечення, а також при наданні керованих послуг та хмарних сервісів. Основні заходи з розробки, включаючи управління конфігурацією та документацією, розробку безпеки та планування життєвого циклу, були впроваджені в практику постачальників продуктів та послуг. Проекти з розробки програмного забезпечення, забезпечення якості апаратного забезпечення, керованих сервісів та хмарної безпеки постійно аналізують важливість стандартів та знижують або підвищують рівень відповідності згідно з рішеннями, заснованими на оцінці ризиків.	Країна бере активну участь у розробці та популяризації цих стандартів на міжнародному рівні. Впровадження цих стандартів та рішення про їх невідповідність приймаються у відповідь на зміну характеру загроз.

Фактор - D 5.2: Засоби контролю безпеки

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Технологічні заходи контролю безпеки	Розуміння та застосування засобів контролю технологічної безпеки, доступних на ринку, користувачами, державним та приватним секторами є мінімальним або взагалі відсутнє. Інтернет-провайдери та інші постачальники технологічних послуг не можуть пропонувати своїм клієнтам будь-які засоби попереднього контролю.	Засоби контролю технологічної безпеки застосовуються користувачами, державним і приватним секторами, але, можливо, не у всіх галузях. Заохочується розгортання сучасних засобів контролю технологічної безпеки, і всі галузі підтримуються у використанні цих засобів. Інтернет-провайдери та інші постачальники технологічних послуг можуть пропонувати послуги безпеки як частину своїх послуг, на спеціальних умовах.	У всіх галузях розгорнуті сучасні засоби контролю технологічної безпеки, включаючи усунення вразлтвостей та резервне копіювання. Для запобігання несанкціонованого доступу персоналу до комп'ютерної техніки в усіх галузях застосовуються засоби фізичного захисту. Інтернет провайдери та інші постачальники послуг встановлюють внутрішню політику щодо розгортання засобів контролю технічної безпеки для управління виявленими ризиками у продуктах та послугах, які вони пропонують. Набір засобів контролю технологічної кібербезпеки відображає встановлені на міжнародному рівні принципи, стандарти та передовий досвід у сфері кібербезпеки.	Широке впровадження засобів контролю технологічної безпеки призводить до ефективного захисту користувачів, державного та приватного секторів. Усі галузі мають можливість постійно оцінювати розгорнуті засоби контролю безпеки на предмет їх ефективності та придатності відповідно до своїх потреб. Розуміння розгорнутих засобів контролю технологічної безпеки охоплює їх вплив на діяльність організації та розподіл бюджетних коштів. Державний та приватний сектори мають можливість критично оцінювати та вдосконалювати засоби контролю кібербезпеки відповідно до їх доцільності та придатності для використання, а також з урахуванням нових ризиків. Широко впроваджується багатофакторна аутентифікація для онлайн-сервісів та привілейованих облікових записів. Функціонують центри сертифікації та широко використовуються цифрові сертифікати. Інтернет провайдери та інші постачальники технологічних послуг мають можливість забороняти доступ до ненадійних сайтів або веб-адрес згідно з вимогами відповідного регуляторного органу.	Застосування передових методів технологічного контролю всередині країни є провідним фактором впливу на міжнародному рівні. Впровадження передових технологічних засобів контролю безпеки здійснюється у відповідь на зміну характеру загроз.

Фактор - D 5.2: Засоби контролю безпеки

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Криптографічний контроль	Криптографічні методи (наприклад, шифрування та цифрові підписи) захисту інформації, що перебуває в стані зберігання та передачі, не застосовуються в державному чи приватному секторі, а також широким загалом.	Криптографічні засоби захисту даних у стані збереження та під час передачі визнаються та впроваджуються несистематично різними зацікавленими сторонами та в різних галузях. TLS, використовується постачальниками послуг для захисту всіх комунікацій між серверами та користувачами.	Криптографічні методи для захисту даних, що перебувають у стані збереження або передачі, доступні для всіх галузей і користувачів. Існує широке розуміння захищеного зв'язку, наприклад, зашифрованої або підписаної електронної пошти. Розгорнуті засоби криптографічного захисту відповідають міжнародним стандартам та керівним принципам для кожної галузі та підтримуються в актуальному стані. TLS, постійно використовується постачальниками послуг для захисту всіх комунікацій між серверами та користувачами.	Державний та приватний сектори критично оцінюють розгортання криптографічного захисту відповідно до своїх цілей та пріоритетів. Державний та приватний сектори адаптують політику шифрування та криптографічного захисту відповідно до розвитку технологічного прогресу та змін у характері загроз. Державний та приватний сектори розробили політику шифрування та криптографічного захисту на основі попереднього оцінювання та регулярно переглядають цю політику на предмет її ефективності. Країна розглядає можливість запровадження управління цифровою ідентичністю. Країна розглянула питання про те, чи потрібна їй національна PKI*.	Країна робить свій внесок у міжнародні дискусії щодо найкращих практик криптографічного захисту інформації. Впровадження засобів криптографічного захисту здійснюється у відповідь на зміну характеру загроз.

* Transport Layer Security
***Інфраструктура відкритих ключів (Public Key Infrastructure)

Фактор - D 5.3: Якість програмного забезпечення

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Гарантія якості програмного забезпечення	Якість та ефективність програмного забезпечення, що використовується в країні, викликає занепокоєння, але функціональні вимоги ще не повністю контролюються. Каталогу перевірених програмних платформ та додатків у державному та приватному секторах не існує. Політики та процеси щодо оновлення та обслуговування (включаючи управління виправленнями) програмних додатків ще не сформульовані.	Якість програмного забезпечення та функціональні вимоги в державному та приватному секторах визнаються та ідентифікуються, але не обов'язково в стратегічному плані. Розробляється каталог перевірених програмних платформ і додатків у державному та приватному секторах. Наразі розробляється політика та процеси щодо оновлення та обслуговування програмного забезпечення (включаючи управління виправленнями). Збираються та оцінюються фактичні дані про виявлені недоліки якості програмного забезпечення та їх вплив на зручність використання та продуктивність.	Визнано та встановлено вимоги до якості та функціональності програмного забезпечення в державному та приватному секторах. Надійні програмні додатки, що відповідають міжнародним стандартам та передовому досвіду, широко використовуються в державному та приватному секторах. В усіх галузях запроваджено політику та процеси оновлення та обслуговування програмного забезпечення (включаючи управління виправленнями). Програмне забезпечення характеризується за надійністю, зручністю використання та продуктивністю відповідно до міжнародних стандартів та найкращих практик.	Контролюється та оцінюється якість програмного забезпечення, яке використовується в державному та приватному секторах. Політики та процеси щодо оновлення та обслуговування програмного забезпечення (включаючи керування виправленнями) удосконалюються на основі оцінки ризиків і критичного характеру послуг у всіх секторах. Вимірюються та оцінюються переваги для бізнесу від додаткових інвестицій у забезпечення якості та обслуговування програмного забезпечення. Дефекти програмного забезпечення своєчасно усуваються та забезпечується безперервність надання послуг.	Доступні програмні додатки високого рівня продуктивності, надійності та зручності використання, з повністю автоматизованими процесами безперервності обслуговування. Вимоги до якості програмного забезпечення систематично переглядаються, оновлюються та адаптуються до мінливого середовища кібербезпеки.

Фактор - D 5.4: Стійкість інфраструктури зв 'язку та Інтернету

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Надійність Інтернет-інфраструктури	Доступні та надійні Інтернет-послуги та інфраструктура в країні, можливо, не були створені; якщо ж вони були створені, то темпи впровадження цих послуг викликають занепокоєння. Державний нагляд за мережевою інфраструктурою є незначним або взагалі відсутній. Якщо мережі та системи передаються на аутсорсинг, надійність сторонніх постачальників може бути не врахована. Заходи з резервування мережі можуть бути розглянуті, але не систематично і не комплексно.	Доступні обмежені Інтернет-послуги та інфраструктура, але з низьким рівнем впровадження та питаннями ненадійності. Багато зацікавлених сторін обговорювали здатність інфраструктури Інтернету в державному та приватному секторах протистояти інцидентам із мінімальними збоями, але, можливо, не повністю розглянули цю тему. Підтримка у питаннях безпеки Інтернет-інфраструктури може спиратися на регіональну допомогу.	Надійні Інтернет-послуги широко доступні та використовуються. Інтернет-послуги користуються широкою довірою для здійснення електронної комерції та електронних ділових операцій; встановлені відповідні процеси автентифікації. Розгорнуті технології та процеси управління інтернет-інфраструктурою відповідають міжнародним стандартам та найкращим практикам. Національна інфраструктура управляється формально, із задокументованими процесами, ролями та обов'язками, з обмеженим резервуванням.	Регулярно проводиться оцінка технологій, процесів на відповідність міжнародним стандартам, а також керівних принципів, які відповідають національним потребам перед обличчям нових ризиків, і за необхідності вносяться зміни. Здійснюється ефективне та контрольоване придбання критичних технологій, запроваджено кероване стратегічне планування та процеси безперервності надання послуг.	Ефективно контролюється придбання інфраструктурних технологій, враховуючи гнучкість до мінливої динаміки ринку. Витрати на інфраструктурні технології постійно аналізуються та оптимізуються. Науково-технічний, промисловий та людський потенціал систематично підтримується, нарощується та примножується з метою підтримання незалежної стійкості країни. Оптимізовано ефективність, щоб запобігти тривалим відключенням систем.
Моніторинг та реагування	Власниками Інтернет-інфраструктури не проводиться оцінка ризиків з метою виявлення вразливих активів та визначення пріоритетності захисних заходів. Відсутній моніторинг для виявлення таких інцидентів. Відсутні плани реагування на інциденти.	Розпочато процеси з розробки оцінки ризиків для власників інтернет-інфраструктури. Існує спеціальний моніторинг елементів Інтернет-інфраструктури, але він може бути не повним. У деяких галузях розробляються плани реагування на інциденти.	Як у державному, так і в приватному секторах існують механізми для проведення оцінки ризиків, моніторингу та тестування стійкості мереж, а також реагування на інциденти. Плани реагування на інциденти існують як у державному, так і в приватному секторах, регулярно тестуються та аналізуються. Відповідні ресурси виділяються на інтеграцію апаратного забезпечення, стрес-тестування технологій, навчання персоналу, моніторинг, реагування та проведення навчань з відпрацювання планів реагування.	Власники Інтернет-інфраструктури регулярно оцінюють ризики, пов’язані з новими та конвергентними технологіями. Ризики, пов'язані з новими та конвергентними технологіями, регулярно оцінюються регуляторними органами, відповідальними за електронні комунікаційні мережі, і використовуються для обґрунтування фінансування та пріоритетних рішень.	Активи національного рівня можуть співпрацювати з міжнародною спільнотою у разі виникнення міжюрисдикційної кризи або інциденту. Досвід міжнародної співпраці використовується для розвитку можливостей моніторингу та реагування. Існують докази того, в очікуванні нових загроз, розвиваються нові можливості моніторингу та реагування на них.

Фактор - D 5.5: Ринок кібербезпеки

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Технології кібербезпеки	Якщо власне виробництво технологій кібербезпеки і існує, то воно не відповідає безпечним процесам. Країна не розглядала безпекові наслідки використання іноземних технологій кібербезпеки. .	Якщо є власне виробництво, визнається потреба у безпечних процесах. Якщо існує залежність від іноземних технологій, враховуються наслідки для безпеки.	Якщо існує власне виробництво, то там налагоджені безпечні процеси. Якщо існує залежність від іноземних технологій, визначаються та пом'якшуються наслідки для безпеки в контексті міжнародного механізму постачання.	Якщо технологія кібербезпеки розробляється локально, то вона дотримується керівних принципів безпечного кодування, кращих практик та відповідає міжнародним стандартам. Оцінка ризиків та ринок впливають на визначення пріоритетів у розробці продуктів та пом'якшення виявлених ризиків. Наслідки використання іноземних технологій для безпеки регулярно аналізуються та переглядаються на основі оцінки нових ризиків у сфері кібербезпеки.	Функції безпеки в програмному забезпеченні та конфігураціях комп'ютерних систем автоматизовані при розробці та розгортанні технологій. Вітчизняна продукція у сфері кібербезпеки експортується до інших країн і вважається високоякісною. В країні створено орган, який забезпечує безпеку іноземних технологій (пристроїв та програмного забезпечення) та шляхів їх постачання, або сертифікує суб'єктів, які можуть це робити.
Консультаційні послуги та експертиза з кібербезпеки	Консультаційні послуги з питань кібербезпеки не є широко доступними в країні. Мало хто з постачальників послуг має професійну сертифікацію.	Зростає кількість консультаційних послуг з кібербезпеки, доступних для приватних та державних організацій. Все більше постачальників послуг надають детальну інформацію про професійні сертифікати, якими вони володіють. Рекомендації для допомоги організаціям у виборі постачальників послуг можуть бути обмеженими або взагалі відсутніми.	Існує широкий спектр консультаційних послуг з питань кібербезпеки, доступних для приватних і державних організацій. Всі постачальники послуг надають детальну інформацію про професійні сертифікати, які вони мають. Державний орган акредитує постачальників послуг, щоб допомогти організаціям у виборі постачальників послуг.	Приватні та державні організації регулярно звертаються до консультаційних служб з питань кібербезпеки, в тому числі за порадами щодо виникаючих ризиків. В країні є достатня кількість фахівців у сфері кібербезпеки.	Сфера послуг з кібербезпеки в країні допомагає формувати міжнародний ринок.

Фактор - D 5.5: Ринок кібербезпеки

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Наслідки аутсорсингу для безпеки	Оцінка ризиків для визначення шляхів зменшення ризиків аутсорсингу IT третім особам або хмарних сервісів не проводиться. Відсутнє розуміння заходів безпеки, які застосовує аутсорсинговий постачальник IT-послуг.	Деякі організації та підприємства проводять оцінку ризиків, щоб визначити, як зменшити ризики, пов'язані з передачею IT на аутсорсинг третім особам або хмарним сервісам. Принаймні деякі організації та підприємства розуміють заходи безпеки, які застосовує постачальник аутсорсингових IT-послуг. Принаймні деякі організації розробили процеси забезпечення безперервності бізнесу та відновлення після катастроф.	Більшість великих організацій державного та приватного секторів проводять оцінку ризиків, щоб визначити, як зменшити ризики передачі IT на аутсорсинг третім особам або хмарним сервісам. Існує розуміння гарантій безпеки, що надаються постачальниками аутсорсингових IT-послуг. Більшість організацій розробили та протестували процеси підтримки безперервності бізнесу та аварійного відновлення.	Висновки, що випливають з оцінки ризиків, регулярно аналізуються з метою запровадження та розповсюдження кращих практик у сфері кібербезпеки для зменшення ризиків аутсорсингу IT. Вивчаються та тестуються різні сценарії ризиків з постачальником IT-послуг, включаючи нові ризики.	Країна робить свій внесок у найкращі міжнародні практики щодо того, як зменшити ризик аутсорсингу IT.
Кібер-страхування	Потреба в ринку кібер-страхування можливо була визначена, але жодні продукти та послуги не доступні ні на внутрішньому ринку, ні від зовнішніх постачальників.	Потреба в ринку кібер-страхування була визначена шляхом оцінки фінансових ризиків для державного та приватного секторів, і зараз обговорюється відповідність існуючих пропозицій.	Створено ринок кібер-страхування, який заохочує обмін інформацією про загрози між учасниками ринку. Також пропонуються продукти, орієнтовані на малі та середні підприємства (МСП).	Ринок кібер-страхування пропонує різні варіанти покриття для мінімізації наслідків можливих збитків. Страхове покриття обирається організаціями на основі потреб стратегічного планування та виявлених ризиків. Ринок кіберстрахування є інноваційним та адаптується до нових ризиків, стандартів та практик, одночасно охоплюючи весь спектр збитків від кібератак. Зниження страхових внесків передбачається за дотримання правил кібербезпеки.	Практики кібер-страхування в країні допомагають формувати міжнародний ринок.

Фактор - D 5.6: Відповідальне оприлюднення даних

Аспект	Початковий етап	Формуючий етап	Етап становлення	Стратегічний етап	Динамічний етап
Обмін інформацією про вразливості	Не існує неформального способу обміну інформацією між зацікавленими сторонами про технічні деталі вразливостей. Постачальники програмного забезпечення та послуг, зазвичай, не мають можливості розглядати повідомлення про помилки та вразливості.	Технічні деталі вразливостей неофіційно передаються іншим зацікавленим сторонам, які можуть поширити цю інформацію. Постачальники програмного забезпечення та послуг можуть розглядати повідомлення про помилки та вразливості, але формальних протоколів для цього не існує. .	Існують офіційні механізми або канали для обміну технічними деталями вразливостей з іншими зацікавленими сторонами, які можуть розповсюдити інформацію широкому загалу. Значна частина вразливостей у продуктах та послугах усувається впродовж визначених термінів після їх виявлення.	Механізми обміну інформацією про вразливості постійно аналізуються та оновлюються з урахуванням потреб усіх зацікавлених сторін, а також з огляду на нові ризики. Усі зазначені продукти та послуги регулярно оновлюються протягом визначеного терміну. Існують процеси для аналізу та скорочення термінів, де це можливо.	Країна робить свій внесок у дискусії та передовий міжнародний досвід щодо обміну інформацією про вразливості.
Політика, процеси та законодавство щодо належного розкриття недоліків системи безпеки	Потреба в політиці щодо належного розкриття інформації в організаціях державного та приватного секторів, а також право на правовий захист для тих, хто розкриває недоліки в системі безпеки, ще не визнані.	Визнається необхідність політики щодо розкриття інформації в організаціях державного та приватного сектору, але така політика або процеси можуть бути відсутніми або перебувати лише на стадії розробки. Визнається право на правовий захист для тих, хто розкриває недоліки безпеки, але законодавство може не діяти або бути на стадії розробки. Постачальники програмного забезпечення та послуг зобов'язуються утримуватися від судових позовів проти сторони, яка відповідально розкриває інформацію.	В організаціях державного та приватного сектору існує політика або система належного розкриття інформації, яка включає в себе кінцевий термін розкриття інформації, заплановане рішення та необхідність підтвердження. Організації запровадили процеси належного отримання та розповсюдження інформації про вразливості. Існує право на правовий захист для тих, хто відповідально розкриває недоліки безпеки.	Політика та процеси розкриття інформації постійно переглядаються та оновлюються відповідно до потреб усіх зацікавлених сторін та з урахуванням нових ризиків. Публікується аналіз технічних деталей вразливостей та поширюється консультативна інформація відповідно до розподілу функцій та обов'язків.	Країна робить свій внесок у дискусії щодо механізмів належного розкриття інформації та правового захисту тих, хто належним чином виявляє недоліки у сфері безпеки.

Еволюція CMM

Це видання CMM 2021 базується на успішності моделі за останні шість років, враховуючи зміни кіберзагроз для користувачів, досвід, отриманий з більш ніж 120 переглядів CMM, проведених по всьому світу, та зворотний зв'язок з експертами в галузі кібербезпеки.

Рішення про перегляд CMM було обумовлено двома ключовими факторами:

- Необхідність реагування на всі відповідні аспекти загроз, вразливості систем і завданої шкоди через зміни в оперативному середовищі та ризики; і
- Переоцінка змін у ландшафті контролю кібербезпеки та практик управління ризиками, доступних для спільноти.

Щоб визначити, чи пропонувати зміни в CMM або в доказах, необхідних для обґрунтування досягнення зрілості потужностей, було застосовано наступний процес прийняття рішень.

Всі потенційні зміни, рекомендовані для включення до видання CMM 2021 року, мали відповідати наступним критеріям:

- Кожна зміна мала бути запропонована партнерами, користувачами чи експертами. Вона має ґрунтуватися на досвіді впровадження моделі, зворотному зв'язку від країни, яка використовувала цю модель, або від члена міжнародної спільноти зацікавлених сторін з особливим розумінням змін у середовищі, які необхідно взяти до уваги;
- Зміни повинні були обговорюватися з Експертно-консультативною групою GCSCC, регіональними, стратегічними партнерами, партнерами по впровадженню, та іншими експертами під час онлайн конференцій та/або індивідуальних онлайн-зустрічей. Серед присутніх має бути досягнутий чіткий і консенсус;
- Ця зміна обговорювалася на семінарі з перегляду CMM у лютому 2020 року. Між учасниками мав бути досягнутий чіткий консенсус;
- Необхідно було провести консультації з партнерами з Global Constellation, стратегічними партнерами та партнерами по реалізації; і
- Члени Технічної ради GCSCC повинні погодитися з тим, що зміни доцільні.

Критерії, які не відповідали вимогам, були задокументовані як такі, що потребують подальших досліджень та консультацій.

Висловлення подяки

This *CMM 2021 Edition* was developed by the GCSCC with significant contributions by its partners and collaborators:

GCSCC Technical Board

GCSCC Research Team

GCSCC Expert Advisory Panel

Global Constellation Partners

- Cybersecurity Capacity Centre for Southern Africa (C3SA), Cape Town, South Africa
- Oceania Cyber Security Centre (OCSC), Melbourne, Australia

Strategic and Implementation Partners

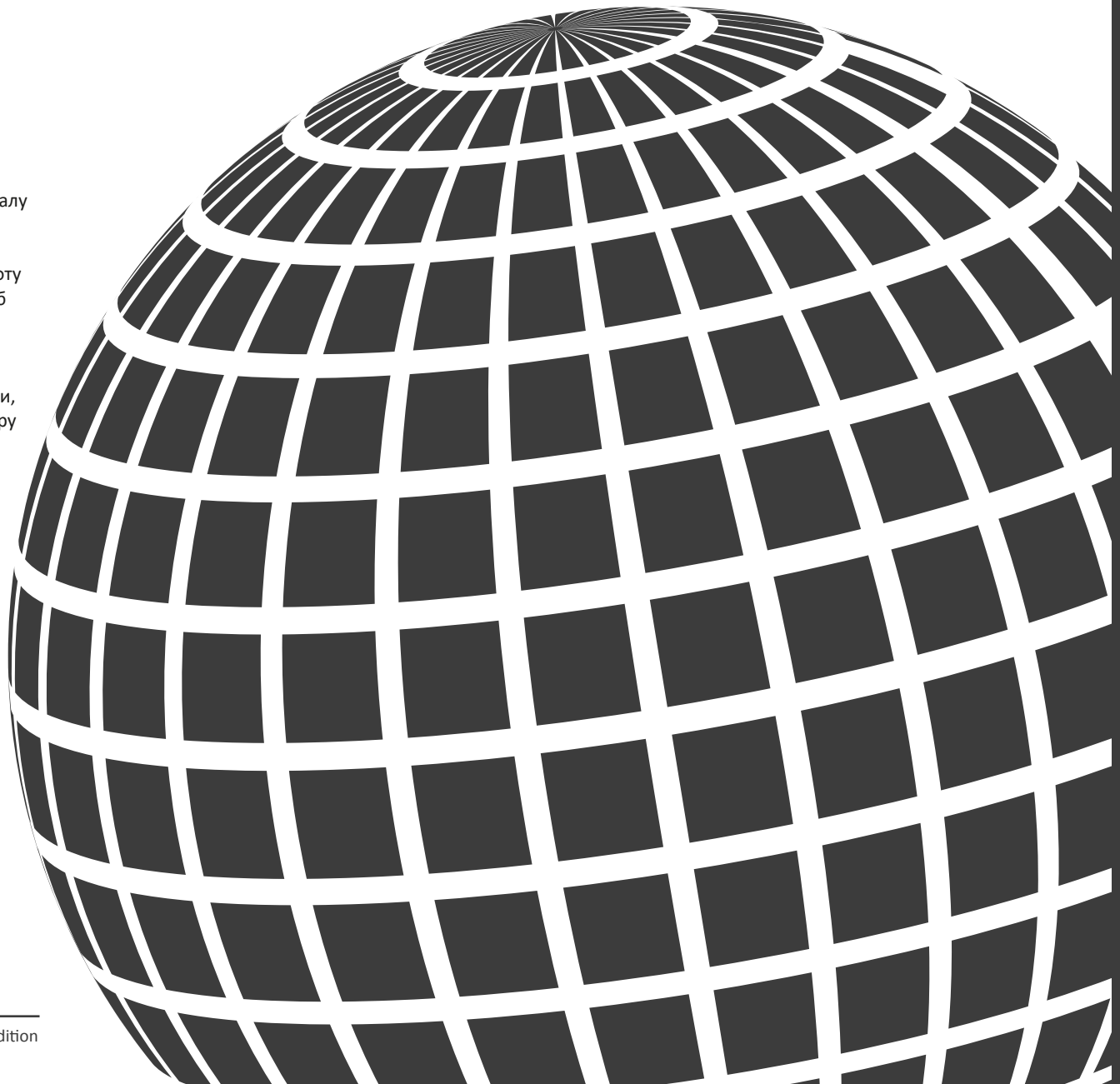
- Commonwealth Telecommunications Organisation (CTO)
- Global Forum on Cyber Expertise (GFCE)
- International Telecommunication Union (ITU)
- NRD Cyber Security
- Organization of American States (OAS)
- World Bank

More than 150 individuals contributed to different steps of the revision process, too many to list them all. We would like to thank all of them.

We also would like to thank our research funders and our partners who provided in-kind support: the UK Foreign, Commonwealth and Development Office (FCDO), State Government of Victoria (Australia), the Organization of American States (OAS), the Inter-American Development Bank (IDB), the World Bank, the International Telecommunications Union (ITU), the Commonwealth Telecommunication Organisation (CTO), the Global Forum on Cyber Expertise (GFCE), the Norwegian Ministry of Foreign Affairs, the Ministry of Foreign Affairs of the Netherlands, GIZ (the German agency for international co-operation), and NRD Cyber Security.

Про GCSCC

Глобальний центр потенціалу кібербезпеки (GCSCC), програма Оксфордської школи Мартіна, що базується на факультеті комп'ютерних наук Оксфордського університету, є провідним міжнародним центром досліджень з розбудови ефективного та дієвого потенціалу у сфері кібербезпеки. Він сприяє збільшенню масштабу, темпів, якості та впливу ініціатив із розбудови потенціалу кібербезпеки в усьому світі та спрямований на покращення масштабу та ефективності розбудови потенціалу кібербезпеки шляхом отримання більш повного та тонкого розуміння ландшафту потенціалу кібербезпеки. Метою GCSCC є забезпечення того, щоб знання та дослідження, зібрані та проведені Центром, могли допомогти країнам у систематичному та ефективному вдосконаленні їхніх спроможностей у сфері кібербезпеки. Допомагаючи в розумінні національного потенціалу кібербезпеки, GCSCC сподівається сприяти розвитку інноваційного кіберпростору на підтримку добробуту, прав людини і процвітання для всіх.



Global
Cyber Security
Capacity Centre

Global Cyber Security Capacity Centre
Department of Computer Science, University of Oxford
Wolfson Building
Parks Road
Oxford
OX1 3QD
United Kingdom

Tel: +44 (0)1865 287430
Email: cybercapacity@cs.ox.ac.uk
Web: https://gcscc.ox.ac.uk/ and https://www.oxfordmartin.ox.ac.uk/cyber-security/

March 2021