EUROPEAN UNION AGENCY
FOR CYBERSECURITY

НАЦИОНАЛНА РАМКА ЗА ОЦЕНКА НА ВЪЗМОЖНОСТИТЕ

ДЕКЕМВРИ 2020 Г.

ЗА ENISA

Агенцията на Европейския съюз за киберсигурност (ENISA) е агенцията на Съюза, насочена към постигане на високо равнище на киберсигурност в цяла Европа. Създадена през 2004 г. и укрепена с Акта за киберсигурността на ЕС, Агенцията на Европейския съюз за киберсигурност допринася за политиката на ЕС в областта на киберсигурността, повишава надеждността на ИКТ продукти, услуги и процеси със схеми за сертифициране на киберсигурността, сътрудничи си с държавите членки и органите на ЕС и помага на Европа да се подготви за бъдещи предизвикателства в областта на киберсигурността. Агенцията работи съвместно с ключовите си партньори — чрез обмен на знания, изграждане на капацитет и повишаване на осведомеността — за повишаване на доверието в свързаната с интернет икономика, за стимулиране на устойчивостта на инфраструктурата на Съюза и в крайна сметка за гарантиране на цифровата сигурност на обществото и гражданите на Европа. За повече информация вж. www.enisa.europa.eu.

ЗА КОНТАКТИ

За да се свържете с авторите, моля използвайте team@enisa.europa.eu.
За медийни запитвания за този документ, моля използвайте press@enisa.europa.eu.

АВТОРИ

Anna Sarri, Pinelopi Kyranoudi – Агенция на Европейския съюз за киберсигурност (ENISA)
Aude Thirriot, Federico Charelli, Yang Dominique - Wavestone

БЛАГОДАРНОСТИ

ENISA би искала да благодари и да признае всички експерти, които са участвали и предоставили ценен принос за този доклад, и по-специално следните, по азбучен ред:

Централна държавна служба за развитие на цифровото общество (Хърватия), Marin Ante Pivcevic

Център за киберсигурност (Белгия)

CFCS — Center for Cybersikkerhed (Дания), Thomas Wulff

Европейски център за борба с киберпрестъпността, Alzofra Martinez Alvaro

Европейски център за борба с киберпрестъпността, Adrian-Ionut Bobeica

Федерално министерство на вътрешните работи (Германия), Sascha-Alexander Lettgen

Администрация за информационна сигурност (Република Словения), Marjan Kavčič

Италианско правителство (Италия)

Малтийска агенция за информационни технологии (Малта), Katia Bonello и Martin Camilleri

Министерство на правосъдието и обществената сигурност (Норвегия), Robin Bakke

Министерство на цифровата политика (Гърция), George Drivas, Nestoras Chouliaras, Evgenia Tsaprali и Sotiris Vasilos

Министерство на икономическите отношения и комуникациите (Естония), Anna-Liisa Pärnalaas

Национална агенция за кибер и информационна сигурност (Чешка република), Veronika Netolická

Национален орган за сигурност (Словакия)

Министерство на националната сигурност (Испания), Maria Mar Lopez Gil

NCTV, Министерство на правосъдието и сигурността (Нидерландия)

Португалски национален център за киберсигурност (Португалия), Alexandre Leite и Pedro atos

Отдел за политика за киберсигурност, Министерство на околната среда, климата и съобщенията (Ирландия), James Caffrey

Оксфордски университет - Глобален център за капацитет за киберсигурност, Carolin Weisser Harris

ENISA също така би искала да благодари за ценния им принос за това проучване, на всички експерти, които предоставиха принос, но предпочитат да останат анонимни.

ПРАВНО УВЕДОМЛЕНИЕ

Трябва да се отбележи, че настоящата публикация представлява становищата и тълкуванията на ENISA, освен ако не е посочено друго. Тази публикация не следва да се тълкува като правно действие на ENISA или органите на ENISA, освен ако не е приета съгласно Регламент (ЕС) 2019/881.
Тази публикация не представлява непременно актуален акт и ENISA може да я актуализира от време на време.
Източниците на трети страни са цитирани според случая. ENISA не носи отговорност за съдържанието на външните източници, включително външните уебсайтове, посочени в настоящата публикация.
Тази публикация е предназначена само за информационни цели. Тя трябва да бъде достъпна безплатно. Нито ENISA, нито което и да е лице, действащо от името на агенцията, носят отговорност за начина на използване на информацията, съдържаща се в настоящата публикация.

ИЗВЕСТИЕ ЗА АВТОРСКО ПРАВО

© Агенция на Европейския съюз за киберсигурност (ENISA), 2020 г.
Възпроизвеждането е разрешено, при условие че източникът е признат.

За използването или възпроизвеждането на снимки или друг материал, който не е авторско право на ENISA, трябва да се иска разрешение пряко от носителите на авторското право.

ISBN: 978-92-9204-475-6

DOI: 10.2824/558701

КАТАЛОГ: TP-02-21-253-BG-N

1. СЪДЪРЖАНИЕ

ТЕРМИНОЛОГИЧЕН РЕЧНИК

АКРОНИМ	ОПРЕДЕЛЕНИЕ
C2M2	Модел за зрялост на капацитета за киберсигурност
CCSMM	Модел за зрялост на киберсигурността на общността
CII	Критична информационна инфраструктура
CMMC	Сертификация на модела за зрялост на киберсигурността
CVD	Координирано разкриване на уязвимост
ECSO	Европейска организация за киберсигурност
GCI	Глобален индекс за киберсигурност
IA-CM	Модел за структура за вътрешен одит за публичния сектор
ISMM	Модел за зрялост на информационната сигурност за рамката за киберсигурност на НИСТ
PET	Технологии за подобряване на защитата на личния живот
Q-C2M2	Модел за зрялост на капацитета за киберсигурност на Катар
ГСС на SOG-IS	Група на старши служители за сигурност на информационните системи, споразумение за взаимно признаване
ДЧ	Държава членка
EACT	Европейска асоциация за свободна търговия
ЕГСКС	Европейска група за сертифициране на киберсигурността
ЕКР	Европейска квалификационна рамка
ЕМКС	Европейския месец на киберсигурността
ЕРИКС	Екипи за реагиране при инциденти с компютърната сигурност
ЕС	Европейски съюз
ЗЗД	Закон за защита на данните
ИИ	Изкуствен интелект
ИКМ	Индекс на кибер мощността
ИКТ	Информационни и комуникационни технологии
МЗК	Модел за зрялост на капацитета за киберсигурност за държавите
МИС	Мрежова и информационна сигурност
МСД	Международен съюз по далекосъобщения
МСП	Малки и средни предприятия

НИРД	Научно-развойна дейност
НИСТ	Национален институт за стандарти и технологии
НСВ	Национални служители за връзка
НСКС	Национални стратегии за киберсигурност
ООУ	Оператори на основни услуги
ОРЗД	Общ регламент за защита на данните
ПО	Правоприлагащ орган
ПЧП	Публично-частни партньорства
СПОК	Споразумение за признаване на общи критерии
СУЛД	Системата за управление на личните данни
ТО	Технология на операциите
ЦЕП	Цифров единен пазар
ЦСП	Цифрова служба на правителството

КРАТКО ИЗЛОЖЕНИЕ

Тъй като настоящото положение с кибер заплахите продължава да се разширява и кибератаките продължават да увеличават интензивността и броя си, държавите членки на ЕС трябва да реагират ефективно чрез по-нататъшно разработване и адаптиране на своите национални стратегии за киберсигурност (НСКС). След публикуването на първите проучвания, свързани с НСКС от ENISA през 2012 г., държавите членки на ЕС и държавите от ЕАСТ постигнаха голям напредък в разработването и прилагането на своите стратегии.

Докладът представя работата, извършена от ENISA за изграждане на национална рамка за оценка на възможностите (НРОВ).

Рамката има за цел да осигури на държавите членки самооценка на равнището им на зрялост чрез оценка на техните цели на НСКС, което ще им помогне да подобрят и изградят възможности за киберсигурност както на стратегическо, така и на оперативно равнище.

В нея се очертава проста представителна гледна точка за равнището на зрялост на киберсигурността на държавата членка. НРОВ е инструмент, който помага на държавите членки за:

- предоставяне на полезна информация за разработване на дългосрочна стратегия (напр. добри практики, насоки);
- помощ за идентифицирането на липсващите елементи в рамките на НСКС;
- помощ за по-нататъшното изграждане на възможности за киберсигурност;
- подкрепя отчетността на политическите действия;
- дава надеждност за широката общественост и международни партньори;
- подкрепа за достъп и подобряване на обществения имидж като прозрачна организация;
- помощ за предвиждане на проблемите, които предстоят;
- помощ за идентифициране на извлечените поуки и най-добрите практики;
- предоставяне на базова линия за капацитета за киберсигурност в целия ЕС с цел улесняване на обсъжданията; както и
- помощ за оценка на националните възможности по отношение на киберсигурността.

Тази рамка беше разработена с подкрепата на експерти по въпросите на ENISA и представители на 19 държави членки и държави от ЕАСТ[1]. Целевата аудитория на този

[1] Интервюирани бяха представители на следните държави членки и държави от ЕАСТ: Белгия, Хърватия, Чехия, Дания, Естония, Германия, Гърция, Унгария, Ирландия, Италия, Лихтенщайн, Малта, Нидерландия, Норвегия, Португалия, Словакия, Словения, Испания, Швеция.

доклад са политиците, експертите и правителствените служители, които отговарят или са ангажирани със създаването, прилагането и оценката на НСКС и, на по-широко равнище, възможностите за киберсигурност.

Националната рамка за оценка на възможностите обхваща 17 стратегически цели и е структурирана около четири основни клъстера:

- Клъстер #1: Управление и стандарти за киберсигурност
  1. Разработване на национален план за действие при извънредни ситуации, свързани с киберсигурността
  2. Установяване на базови мерки за сигурност
  3. Осигуряване на цифрова идентичност и изграждане на доверие в цифровите обществени услуги

- Клъстер #2: Изграждане на капацитет и осведоменост
  4. Организиране на дейности по киберсигурност
  5. Създаване на възможности за реагиране при инциденти
  6. Повишаване на осведомеността на потребителите
  7. Засилване на обучението и образователните програми
  8. Насърчаване на научно-изследователска и развойна дейност
  9. Осигуряване на стимули за частния сектор за инвестиции в мерки за сигурност
  10. Подобряване на киберсигурността на веригата за доставки

- Клъстер #3: Правни и регулаторни въпроси
  11. Защита на критичната информационна инфраструктура, ООУ и доставчик на цифрови услуги
  12. Справяне с кибер престъпленията
  13. Създаване на механизми за докладване на инциденти
  14. Укрепване на неприкосновеността на личния живот и защитата на данните

- Клъстер #4: Сътрудничество
  15. Създаване на публично-частно партньорство
  16. Институционализиране на сътрудничеството между публичните агенции
  17. Участие в международно сътрудничество

1. ВЪВЕДЕНИЕ

Директивата за мрежова и информационна сигурност (ДМИС), публикувана през юли 2016 г., изисква държавите членки на ЕС да приемат национална стратегия за сигурността на мрежовите и информационните системи, наричана също НСКС (Национална стратегия за киберсигурност), както е предвидено в членове 1 и 7. В този контекст НСКС е дефинирана като рамка, която определя стратегически принципи, насоки, стратегически цели, приоритети, подходящи политики и регулаторни мерки. Предвидената цел на НСКС е да достигне и поддържа високо равнище на мрежова и системна сигурност, като по този начин дава възможност на държавите членки да намалят потенциалните заплахи. Освен това НСКС може да бъде и катализатор за индустриалното развитие и икономически и социален напредък.

В Акта за киберсигурността на ЕС се посочва, че ENISA насърчава разпространението на най-добри практики при определянето и прилагането на НСКС, като подпомага държавите членки при приемането на Директивата за мрежова и информационна сигурност и като събира ценна обратна информация за техния опит. За тази цел ENISA разработи няколко инструмента за подпомагане на държавите членки при разработването, прилагането и оценката на техните национални стратегии за киберсигурност (НСКС).

Като част от своя мандат ENISA има за цел да разработи национална рамка за самооценка на възможностите за измерване на равнището на зрялост на различните НСКС. Целта на доклада е да представи проучването, проведено при определението на рамката за самооценка.

1.1 ОБХВАТ И ЦЕЛИ НА ПРОУЧВАНЕТО

Основната цел на това проучване е да създаде национална рамка за самооценка на възможностите, наричана по-долу НРОВ, за измерване на равнището на зрялост на възможностите за киберсигурност на държавите членки. По-конкретно, рамката следва да оправомощава държавите членки за:

- извършване на оценка на техните национални възможности за киберсигурност.
- повишаване на осведомеността за равнището на зрялост на държавата;
- определяне на областите за подобряване; както и
- изграждане на възможности за киберсигурност.

Тази рамка следва да помогне на държавите членки, и по-специално на националните политици, да извършат самооценка с цел подобряване на националните възможности за киберсигурност.

1.2 МЕТОДОЛОГИЧЕН ПОДХОД

Методологическият подход, използван за разработване на рамката за самооценка на националните възможности, се основава на четири основни стъпки:

1. **Проучване на бюро**: Първата стъпка включваше провеждането на обширен литературен преглед с цел събиране на най-добри практики по отношение на разработването на рамка за оценка на зрялостта на националните стратегии за киберсигурност. Проучването на бюро е насочено към систематичен анализ на съответните документи за изграждане на капацитет и определяне на стратегия за

киберсигурност, върху съществуващите НСКС на държавите членки и върху сравнение на съществуващите модели на зрялост относно киберсигурността. Въвеждането на референтна стойност на съществуващите модели за зрялост беше извършено чрез приемането на рамка за анализ, разработена за целите на настоящото проучване. Рамката на анализ се основава на методологията на Becker[2] за разработване на модели за зрялост, която определя общ и консолидиран модел на процедура за създаване на модели за зрялост и осигурява ясни изисквания за разработването на модели за зрялост. Рамката на анализа беше допълнително настроена, за да отговори на нуждите на това проучване.

2. **Събиране на гледните точки на експертите и заинтересованите страни**: Въз основа на данните, събрани чрез проучване на бюро и свързаните предварителни констатации от анализа, тази фаза включваше идентифициране и покана за интервю на идентифицираните експерти, които имат опит в разработването и изпълнението на НСКС или на модели за зрялост. ENISA се свърза със своята експертна група за национални стратегии за киберсигурност и националните служители за връзка (НСВ), за да намери съответните експерти във всяка държава членка. Освен това бяха интервюирани някои експерти, които участват в разработването на модели за зрялост. Като цяло бяха проведени 22 интервюта, 19 от които бяха с представители на агенциите за киберсигурност в различните държави членки (и държавите от ЕАСТ).

3. **Анализ на входящите данни за проверка:** Данните, събрани чрез проучване на бюро и интервютата впоследствие бяха анализирани за идентифициране на най-добрите практики при създаването на рамка за самооценка за измерване на зрелостта на НСКС, за разбиране на потребностите на държавите членки и за определяне кои данни могат да бъдат събрани в различните европейски държави[3]. Този анализ даде възможност за прецизиране на предварителния модел, разработен в предходните стъпки, както и за усъвършенстване на набора от показатели, включени в модела, нивата на зрялост и неговите измерения.

4. **Завършване на модела:** След това актуализирана версия на рамката за самооценка на националните възможности бе преразгледана от експертите по въпросите на ENISA и след това допълнително потвърдена от експерти на семинар, проведен през октомври 2020 г. преди публикуването.

1.3 ЦЕЛЕВА АУДИТОРИЯ

Целевата аудитория на този доклад са политиците, експертите и правителствените служители, които отговарят или са ангажирани със създаването, прилагането и оценката на НСКС и, на по-широко равнище, възможностите за киберсигурност. Освен това констатациите, формализирани в този документ, могат да бъдат от полза за експертите и изследователите в областта на киберсигурността на национално или европейско равнище.

[2] J. Becker, R. Knackstedt, и J. Pöppelbuß, „Разработване на модели на зрялост за управление на ИТ: Процедурен модел и неговото приложение," Business & Information Systems Engineering, том 1, № 3, стр. 213—222, юни 2009 г.
[3] За целите на това проучване „европейските държави", посочени в настоящия доклад, включват 27-те държави членки на ЕС.

2. КОНТЕКСТ

2.1 ПРЕДИШНА РАБОТА ПО ЖИЗНЕНИЯ ЦИКЪЛ НА НСКС

Както е посочено в Акта за киберсигурността на ЕС, една от основните цели на ENISA е да подкрепи държавите членки при разработването на национални стратегии за сигурността на мрежовите и информационните системи, да насърчава разпространението на тези стратегии и да наблюдава тяхното прилагане. Като част от своя мандат ENISA представи няколко документа по този въпрос, за да насърчи споделянето на добри практики и да подкрепи прилагането на НСКС в целия ЕС:

- „Практически наръчник за фазата на развитие и изпълнение на НСКС“[4] , публикуван през 2012 г.
- „Определяне на курса за национални усилия за укрепване на сигурността в киберпространството“[5] , публикувана през 2012 г.
- Първата рамка на ENISA за оценка на НСКС на държава членка, публикувана[6] през 2014 г.
- „Онлайн интерактивна карта за НСКС“[7] , публикувана през 2014 г.
- „Наръчник за добри практики на НСКС“[8] , публикуван през 2016 г.
- „Национален инструмент за оценка на стратегиите за киберсигурност“[9] , публикуван през 2018 г.
- „Добри практики в иновациите в областта на киберсигурността в рамките на НСКС“[10] , публикувани през 2019 г.

ПРИЛОЖЕНИЕ А представя кратко резюме на основните публикации на ENISA по тази тема.

Гореспоменатите ръководства и документи бяха проучени като част от проучването на бюро. По-специално, „Националният инструмент за оценка на стратегиите за киберсигурност“[11] е основен елемент на НРОВ. НРОВ се основава на целите, обхванати в онлайн инструмента за оценка на НСКС.

---

[4] НСКС: Практическо ръководство за развитие и изпълнение (ENISA, 2012 г.)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[5] НСКС: Определяне на курса за национални усилия за укрепване на сигурността в киберпространството (ENISA, 2012 г.)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[6] Рамка за оценка за НСКС (ENISA, 2014 г.)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[7] Национални стратегии за киберсигурност — Интерактивна карта (ENISA, 2014 г., актуализирана през 2019 г.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[8] Настоящият документ актуализира ръководството от 2012 г. Наръчник за добри практики на НСКС: Създаване и прилагане на национални стратегии за киберсигурност (ENISA, 2016 г.)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[9] Национален инструмент за оценка на стратегиите за киберсигурност (2018 г.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[10] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1
[11] Национален инструмент за оценка на стратегиите за киберсигурност (2018 г.)
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

2.2 ОБЩИ ЦЕЛИ, ОПРЕДЕЛЕНИ В РАМКИТЕ НА ЕВРОПЕЙСКАТА НСКС

Несъответствието между различните държави членки затруднява идентифицирането на общи дейности или планове за действие между различните национални контексти, правни рамки и политически дневен ред. Все пак, НСКС на държавите членки често имат стратегически цели, които са формулирани по едни и същи теми. По този начин, въз основа на предишната работа на ENISA и на анализа на НСКС на държавите членки бяха установени 22 стратегически цели. 15 от тези стратегически цели вече бяха определени в предишната работа на ENISA, 2 бяха добавени наново в това проучване и бяха определени 5 цели за бъдещи съображения.

2.2.1 Общи стратегически цели, обхванати от държавите членки

Въз основа на предишната работа на ENISA, а именно инструмента за оценка на националните стратегии за киберсигурност[12], таблицата по-долу показва гореспоменатия набор от 15 стратегически цели, които обикновено са обхванати в НСКС на държавите членки. Целите очертават същността на цялостната „национална философия“ по темата. За допълнителна информация относно целите, описани по-долу, моля, обърнете се към доклада на ENISA „Наръчник за добри практики на НСКС“.[13]

Таблица1: Общи стратегически цели, обхванати от държавите членки в техните НСКС

Реф. номер	Стратегически цели на НСКС	Цели
1	**Разработване на национални планове за действие при извънредни ситуации, свързани с киберсигурността**	▶ Представяне и обясняване на критериите, които следва да се използват за определяне на дадена ситуация като криза; ▶ Определяне на ключови процеси и действия за справяне с кризата; и ▶ Ясно определяне на ролите и отговорностите на различните заинтересовани страни по време на киберкризата. ▶ Представяне и обясняване на критериите за край на една криза и/или кой има право да го заявява.
2	**Установяване на базови мерки за сигурност**	▶ Хармонизиране на различните практики, следвани от организациите както в публичния, така и в частния сектор; ▶ Създаване на общ език между компетентните публични органи и организациите и отворените сигурни комуникационни канали; ▶ Позволяване на различните заинтересовани страни да проверяват и сравняват своите възможности за киберсигурност; ▶ Споделяне на информация за добрите практики при киберсигурността във всеки сектор на промишлеността; и ▶ Помощ на заинтересованите страни да определят по приоритет инвестициите си в областта на сигурността.
3	**Организиране на дейности по киберсигурност**	▶ Идентифициране на това, което трябва да бъде изпитвано (планове и процеси, хора, инфраструктура, възможности за реагиране, възможности за сътрудничество, комуникация и др.); ▶ Създаване на национален екип за планиране на дейности, свързани с киберсигурността с ясен мандат; и ▶ Интегриране на свързаните с киберсигурност дейности в рамките на жизнения цикъл на националната стратегия за киберсигурност

https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

[12] Национален инструмент за оценка на стратегиите за киберсигурност (2018 г.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool

[13] Настоящият документ актуализира ръководството от 2012 г. Наръчник за добри практики на НСКС: Създаване и прилагане на национални стратегии за киберсигурност (ENISA, 2016 г.)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Реф. номер	Стратегически цели на НСКС	Цели
		или националния план за действие при извънредни ситуации, свързани с киберсигурност.
4	Създаване на възможности за реагиране при инциденти	▶ Мандат — той се отнася до правомощията, ролите и отговорностите, които трябва да бъдат разпределени на екипа от съответното правителство; ▶ Портфолио от услуги — то обхваща услугите, които екипът предоставя на своите клиенти или използва за собственото си вътрешно функциониране; ▶ Оперативни възможности — това се отнася до техническите и оперативните изисквания, които екипът трябва да спазва; и ▶ Възможности за сътрудничество — те обхващат изисквания по отношение на обмена на информация с други екипи, които не са обхванати от предходните три категории, напр. политици, военни, регулатори, оператори (на критична информационна инфраструктура), правоприлагащи органи.
5	Повишаване на осведомеността на потребителите	▶ Идентифициране на пропуските в знанията по въпросите на киберсигурността или информационната сигурност; и ▶ Отстраняване на пропуските чрез повишаване на осведомеността или разработване/укрепване на основите на знанието.
6	Засилване на обучението и образователните програми	▶ Повишаване на оперативните възможности на съществуващата работна сила в областта на информационната сигурност; ▶ Насърчаване на учениците да се присъединят и след това да бъдат подготвени да навлязат в областта на киберсигурността; ▶ Стимулиране и насърчаване на отношенията между академичната среда в областта на информационната сигурност и промишлеността на информационната сигурност; и ▶ Синхронизиране на обучението по киберсигурност с нуждите на бизнеса.
7	Насърчаване на научно-изследователска и развойна дейност	▶ Идентифициране на реалните причини за уязвимите места, вместо поправяне на тяхното въздействие; ▶ Обединяване на учени от различни дисциплини за осигуряване на решения на многоизмерни и сложни проблеми като физически кибер заплахи; ▶ Обединяване на нуждите на промишлеността и констатациите от научните изследвания, като по този начин се улеснява прехода от теория към практика; и ▶ Намиране на начини не само за поддържане, но и за увеличаване на нивото на киберсигурност на продуктите и услугите, които подкрепят съществуващите кибер инфраструктури.
8	Осигуряване на стимули за частния сектор за инвестиции в мерки за сигурност	▶ Определяне на възможни стимули за частните дружества да инвестират в мерки за сигурност; и ▶ Предоставя на дружествата стимули за насърчаване на инвестициите в сигурността.
9	Защита на критичната информационна инфраструктура, ООУ и доставчик на цифрови услуги (критична информационна инфраструктура)	▶ Идентифициране на критичната информационна инфраструктура; и ▶ Идентифициране и смекчаване на съответните рискове за критична информационна инфраструктура.
10	Справяне с кибер престъпленията	▶ Създаване на закони в областта на киберпрестъпността; и ▶ Повишаване ефективността на правоприлагащите органи.
11	Създаване на механизми за докладване на инциденти	▶ Получаване на знания за цялостната среда на заплахата; ▶ Оценка на въздействието на инциденти (напр. нарушения на сигурността, повреди в мрежата, прекъсвания на услугата); ▶ Получаване на знания за съществуващи и нови уязвими места и видове атаки; ▶ Съответно актуализиране на мерките за сигурност; и ▶ Прилагане на разпоредбите на Директива за мрежова и информационна сигурност относно докладването на инциденти.

Реф. номер	Стратегически цели на НСКС	Цели
12	**Укрепване на неприкосновеността на личния живот и защитата на данните**	▶ Допринасяне за укрепването на основните права относно неприкосновеността на личния живот и защитата на данните.
13	**Създаване на публично-частно партньорство (ПЧП)**	▶ Възпиране (за възпиране на нападателите); ▶ Защита (използване на проучвания на нови заплахи за сигурността); ▶ Откриване (използване на обмена на информация за справяне с нови заплахи); ▶ Реагиране (осигуряване на възможност за справяне с първоначалното въздействие на инцидент); и ▶ Възстановяване (осигуряване на възможност за поправяне на крайното въздействие на инцидент).
14	**Институционализиране на сътрудничеството между публичните агенции**	▶ Увеличаване на сътрудничеството между публичните агенции с отговорности и компетенции, свързани с киберсигурността; ▶ Избягване на припокриването на компетенциите и ресурсите между публичните агенции; и ▶ Подобряване и институционализиране на сътрудничеството между публичните агенции в различни области на киберсигурността.
15	**Участие в международно сътрудничество (не само с държавите членки на ЕС)**	▶ Възползване от създаването на обща база от знания между държавите членки на ЕС; ▶ Създаване на синергичен ефект между националните органи за киберсигурност; и ▶ Предоставяне на възможност и увеличаване на борбата срещу транснационалната престъпност.

2.2.2 Допълнителни стратегически цели

Въз основа на извършеното проучване на бюро и проведените от ENISA интервюта бяха определени допълнителни стратегически цели. Държавите членки все повече се занимават с тези теми в своите НСКС или определят планове за действие по един и същ въпрос. Представени са и примери за дейности, изпълнявани от държавите членки. Ако примерът е от общественодостъпен източник, се предоставя препратка. В случаите, когато примерите се основават на поверителни интервюта с длъжностните лица на държавите - членки на ЕС, не са предоставени източници.

Бяха определени следните допълнителни стратегически цели:

- Подобряване на киберсигурността на веригата за доставки; и
- Осигуряване на цифрова идентичност и изграждане на доверие в цифровите обществени услуги.

Подобряване на киберсигурността на веригата за доставки

Малките и средните предприятия (МСП) са гръбнакът на европейската икономика. Те представляват 99 % от всички предприятия в ЕС[14] и през 2015 г. беше изчислено, че МСП са създали около 85 % от новите работни места и са предоставили две трети от общата заетост на частния сектор в ЕС. Освен това, тъй като МСП предоставят услуги на големи дружества и все повече работят с публичните администрации[15], трябва да се отбележи, че в днешния взаимосвързан контекст МСП представляват слабото звено за кибератаки. Всъщност МСП са най-уязвими на кибер атаки, но често не могат да си позволят да инвестират адекватно в киберсигурност[16]. Следователно подобряването на киберсигурността на веригата за доставки следва да се извършва с акцент върху МСП.

В допълнение към този системен подход държавите членки могат също така да подчертаят усилията по отношение на киберсигурността на конкретни ИКТ услуги и продукти, които се считат за съществени: ИКТ технологиите, използвани в критичната информационна инфраструктура, механизмите за сигурност, прилагани в далекосъобщителния сектор (контроли на ниво ISP...), доверителни услуги, както са определени в Регламента относно електронната идентификация и удостоверителните услуги (Регламента eIDAS) и доставчиците на облачни услуги. Например, в своята национална стратегия[17] за киберсигурност за периода 2019—2024 г. Полша се ангажира да разработи национална система за оценка на киберсигурността и сертифицирането като механизъм за гарантиране на качеството във веригата за доставки. Тази система за сертифициране ще бъде приведена в съответствие с рамката на ЕС за сертифициране за ИКТ цифрови продукти, услуги и процеси, създадена с Акта за киберсигурността на ЕС (2019/881).

Следователно подобряването на киберсигурността на веригата за доставки е от първостепенно значение. Това може да бъде постигнато чрез установяване на силни политики за насърчаване на МСП, предоставяне на насоки за изискванията за киберсигурност в процедурите за възлагане на обществени поръчки на публичната администрация, насърчаване на сътрудничеството в частния сектор, изграждане на ПЧП, насърчаване на координирани механизми за разкриване на уязвимост (CVD)[18], изграждане на схема за сертифициране на продукти, включително компоненти на киберсигурността в цифровите инициативи за МСП, както и финансиране на развитието на умения, наред с другото.

Осигуряване на цифрова идентичност и изграждане на доверие в цифровите обществени услуги

През февруари 2020 г. Комисията изложи визията си за дигиталната трансформация на ЕС в съобщението „Оформяне на дигиталното бъдеще на Европа“[19], с цел предоставяне на приобщаващи технологии, които работят за хората и зачитат основните ценности на ЕС. По-специално в съобщението се посочва, че насърчаването на дигиталната трансформация на публичните администрации в цяла Европа е от решаващо значение. В този смисъл изграждането на доверие в правителството във връзка с цифровата идентичност и доверието в обществените услуги е от първостепенно значение. Това е още по-важно, когато се има предвид факта, че сделките в публичния сектор и обменът на данни често са с чувствителен характер.

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

Много държави са изразили намерението си да разгледат тази тема в своята НСКС, като например: Дания, Естония, Франция, Люксембург, Малта, Испания, Холандия и Обединеното кралство. От тези държави някои заявиха също, че тази стратегическа цел може да бъде разгледана като част от по-широк план:

- Естония свързва своя съответен план за действие относно „Сигурността на електронната идентичност и възможностите за електронно удостоверяване“ с по-широката Цифрова програма за 2020 г. за Естония.
- Френската НСКС посочва, че държавният секретар, който отговаря за цифровите технологии, наблюдава създаването на пътна карта „за защита на цифровия живот, неприкосновеността на личния живот и личните данни на французите“.
- В НСКС на Нидерландия се посочва, че киберсигурността в публичните администрации, както и обществените услуги, предоставяни на гражданите и предприятията, са обсъдени по-подробно в Широка програма за цифрово правителство.
- Тъй като правителството на Обединеното кралство продължава да предоставя повече от своите услуги онлайн, то е определило Цифрова служба на правителството (ЦСП) за гарантиране, че всички нови цифрови услуги, създадени или закупени от правителството, също са „сигурни по подразбиране“, с подкрепата на Британския национален център за киберсигурност (НЦКС).

2.2.3 Други разглеждани стратегически цели

По време на етапа на проучването на бюро и като част от интервютата, проведени от ENISA, бяха проучени и други стратегически цели. Все пак, беше решено, че тези цели няма да са част от рамката за самооценка. ПРИЛОЖЕНИЕ В — Други изследвани цели

предоставя определения за всяка от тези цели, които могат да бъдат използвани за насърчаване на бъдещи дискусии за възможни подобрения на НСКС.

Като бъдещи съображения бяха проучени следните стратегически цели:

- разработване на специфични за сектора стратегии за киберсигурност.
- борба срещу кампаниите за дезинформация.
- сигурни авангардни технологии (5G, изкуствен интелект, квантови изчисления...);
- гарантиране на суверенитета на данните; и
- осигуряване на стимули за развитието на индустрията на киберзастраховането.

2.3 КЛЮЧОВИ ИЗВОДИ ОТ СРАВНЕНИЕТО

Проучването на екран на съществуващите модели на зрялост, свързани с киберсигурността, беше проведено с цел събиране на информация и доказателства в подкрепа на създаването на национална рамка за самооценка на възможностите в областта на НСКС. В този контекст бе извършен обширен литературен преглед на съществуващите модели за допълване на констатациите от първоначалното проучване на обхвата на моделите на зрялост на киберсигурността и съществуващите НСКС, разработени в раздели 2.1 и 2.2. Този систематичен преглед подкрепя подбора и обосновката на нивата на зрялост на рамката за оценка и определянето на различните измерения и показатели.

В рамките на системния преглед на моделите на зрялост бяха разгледани и анализирани 10 модела въз основа на техните основни характеристики. Глобалният преглед на ключовите характеристики за всеки разгледан модел в обхвата на това проучване е

представен в Таблица2: Преглед на анализираните модели на **зрялост** и може да се намери по-подробен анализ в ПРИЛОЖЕНИЕ А.

Таблица2: Преглед на анализираните модели на зрялост

Име на модела	# на нивата на зрялост	# на атрибутите	Метод на оценка	Представяне на резултатите
Модел за зрялост на капацитета за киберсигурност за държавите (M3K)	5	5 основни измерения	Сътрудничество с местна организация за усъвършенстване на модела преди прилагането му в националния контекст	Радар от 5-секции
Модел за зрялост на капацитета за киберсигурност (C2M2)	4	10 основни области	Методология за самооценка и инструментариум	Карта за оценка с диаграми „пай“
Рамка за подобряване на киберсигурността на критичната инфраструктура	Без приложение (4 реда)	5 основни функции	Самооценка	Без приложение
Модел за зрялост на капацитета за киберсигурност на Катар (Q-C2M2)	5	5 основни области	Без приложение	Без приложение
Сертификация на модела за зрялост на киберсигурността (CMMC)	5	17 основни области	Оценка от одитори трети страни	Без приложение
Моделът за зрялост на киберсигурността на общността (CCSMM)	5	6 основни измерения	Оценка в рамките на общностите с принос от държавни и федерални правоприлагащи органи	Без приложение
Модел за зрялост на информационната сигурност за рамката за киберсигурност на НИСТ (ISMM)	5	23 оценени области	Без приложение	Без приложение
Модел за структура за вътрешен одит (IA-CM) за публичния сектор	5	6 елемента	Самооценка	Без приложение
Глобален индекс за киберсигурност (GCI)	Без приложение	5 стълба	Самооценка	Таблица за класиране
Индекс на кибер мощността (ИКМ)	Без приложение	4 категории	Сравнителен анализ на the Economist Intelligence Unit	Таблица за класиране

Този систематичен преглед даде възможност да се направят изводи относно най-добрите практики, приети в съществуващите модели, за подпомагане на разработването на концептуален модел за настоящия модел за зрялост. По-специално въвеждането на референтна стойност подкрепи определянето на нивата на зрялост, създаването на клъстери от измерения и подбора на показатели, както и подходяща методология за показване на резултатите от модела. Най-подходящите констатации за всеки от тези елементи са подробно описани в Таблица 3.

Таблица 3: Ключови изводи от сравнението

Функция	Ключов извод
Нива на зрялост	▶ Обикновено се приема скала за зрялост на пет нива за рамки за оценка на възможностите за киберсигурност и може да предостави резултати от детайлна оценка (вж. Таблица 6 Сравняване на нивата на зрялост за изчерпателно мнение за определянето на нивата на зрялост за всеки модел); ▶ Всички модели предоставят определение на високо равнище на всяко ниво на зрялост, което след това се адаптира към различните измерения или клъстери от измерения; ▶ Два основни аспекта обикновено се оценяват при измерване на зрелостта на възможностите за киберсигурност: зрялост на стратегиите и зрялост на процесите, въведени за прилагане на стратегии.
Атрибути	▶ Сравнителният анализ на атрибутите на съществуващите модели на зрялост показва хетерогенни резултати със среден брой атрибути за модел между четири и пет; ▶ Модел, основаващ се на около четири или пет атрибута, осигурява на държавите правилното ниво на детайлност на данните, като групира съответните измерения заедно и гарантира четливостта на резултатите (вж. Таблица 7: Сравнение на атрибути/ измерения за описание на атрибутите за всеки модел); ▶ Ключовият принцип, приет от всички модели при определянето на клъстерите, се основава на последователността на елементите, групирани във всеки клъстер.
Метод на оценка	▶ Методите за оценка, използвани в различните анализирани модели, се различават един от друг; ▶ Най-често срещаният метод за оценка се основава на самооценка.
Представяне на резултатите	▶ Важно е резултатите да бъдат представени на различно ниво на детайлност; ▶ Методологията за визуализация следва да бъде самообяснителна и лесна за четене.

Концептуалният модел е изграден въз основа на сравнителния анализ на различните модели на зрялост, както и на предишната работа от ENISA. Също така беше решено да се надгради *онлайн интерактивния инструмент на ENISA* за разработване на показатели за зрялост, използвани за всеки атрибут.

2.4 ПРЕДИЗВИКАТЕЛСТВА ПРИ ОЦЕНКАТА НА НСКС

Държавите членки са изправени пред много предизвикателства, когато изграждат възможности за киберсигурност и по-конкретно, когато гарантират, че техните възможности отговарят на последните развития. По-долу е представено обобщение на предизвикателствата, определени и обсъждани с държавите членки като част от настоящото проучване:

- **Трудности при координацията и сътрудничеството:** Координирането на усилията за киберсигурност на национално равнище с цел ефективен отговор на въпросите, свързани с киберсигурността, може да се окаже предизвикателство поради големия брой заинтересовани страни.
- **Липса на ресурси за извършване на оценката:** В зависимост от местния контекст и структурата за управление на киберсигурността на държавата, оценката на НСКС и нейните цели може да отнеме повече от 15 дни за всеки отделен служител.
- **Липса на подкрепа за развитие на възможности за киберсигурност:** Някои държави членки споделиха, че за да защитят бюджета и за да получат подкрепа

за разработването на възможности за киберсигурност, първо трябва да извършат фаза на оценка за установяване на пропуските и ограниченията.

- **Трудности при внасянето на успехи или промени в стратегията:** С развитието на заплахите всеки ден и подобряването на технологиите, в отговор плановете за действие постоянно трябва да бъдат адаптирани. Въпреки това, оценката на НСКС и внасянето на промени в самата стратегия остава трудна задача. Това от своя страна затруднява идентифицирането на ограниченията и недостатъците на НСКС.
- **Трудности при измерване на ефективността на НСКС:** Показателите могат да бъдат събрани за измерване на различни области, като напредък, изпълнение, зрялост и ефективност. Докато измерването на напредъка и изпълнението е относително лесно в сравнение с измерването на ефективността, последното остава по-значимо за оценка на резултатите и въздействията на НСКС. Въз основа на проведените от ENISA интервюта голям брой държави членки заявиха, че количественото измерване на ефективността на НСКС е важно, но също така представлява много трудна задача, която в някои случаи е определено невъзможна.
- **Трудност при приемане на обща рамка:** Държавите членки на ЕС действат в различен контекст по отношение на политиката, организации, култура, структура на обществото и зрялост на НСКС. Някои държави членки, интервюирани като част от това проучване, заявиха, че може да се окаже трудно да се защити и използва рамка за самооценка „един размер“.

2.5 ПОЛЗИ ОТ ОЦЕНКА НА НАЦИОНАЛНИТЕ ВЪЗМОЖНОСТИ

От 2017 г. всички държави членки на ЕС имат НСКС[20]. Макар и положително развитие, важно е също така държавите членки да могат правилно да оценят тези НСКС, като по този начин придават добавена стойност на своето стратегическо планиране и изпълнение.

Една от целите на националната рамка за оценка на възможностите е да се оценят възможностите за киберсигурност въз основа на приоритетите, посочени в различните НСКС. Основно рамката оценява степента на зрялост на възможностите за киберсигурност на държавите членки в областите, определени от целите на НСКС. По този начин резултатите от рамката подкрепят политиците на държавите членки при определянето на националната стратегия за киберсигурност, като им предоставят информация за състоянието на държавата[21]. В крайна сметка НРОВ има за цел да помогне на държавите членки да определят области на подобряване и изграждане на възможности.

Рамката има за цел да осигури на държавите членки самооценка на равнището им на зрялост чрез оценка на техните цели на НСКС, което ще им помогне да подобрят и изградят възможности за киберсигурност както на стратегическо, така и на оперативно равнище.

При по-практичен подход, основан на проведените от ENISA интервюта с няколко агенции, които отговарят за областта на киберсигурността в различни държави членки, бяха установени и подчертани следните ползи от националната рамка за оценка на възможностите:

[20] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[21] Weiss, C.H. (1999 г.). Интерфейс между оценяването и обществената политика. Оценка, 5(4), 468-486.

- предоставяне на полезна информация за разработване на дългосрочна стратегия (напр. добри практики, насоки);
- помощ за идентифицирането на липсващите елементи в рамките на НСКС;
- помощ за по-нататъшното изграждане на възможности за киберсигурност;
- подкрепя отчетността на политическите действия;
- дава надеждност за широката общественост и международни партньори;
- подкрепа за достъп и подобряване на обществения имидж като прозрачна организация;
- помощ за предвиждане на проблемите, които предстоят;
- помощ за идентифициране на извлечените поуки и най-добрите практики;
- предоставяне на базова линия за капацитета за киберсигурност в целия ЕС с цел улесняване на обсъжданията; както и
- помощ за оценка на националните възможности по отношение на киберсигурността.

3. МЕТОДОЛОГИЯ НА НАЦИОНАЛНАТА РАМКА ЗА ОЦЕНКА НА ВЪЗМОЖНОСТИТЕ

3.1 ОБЩА ЦЕЛ

Основната цел на НРОВ е да измери нивото на зрялост на възможностите за киберсигурност на **държавите членки**, за да им окаже подкрепа при извършването на оценка на техните национални възможности за киберсигурност, повишаване на осведомеността за нивото на зрялост на държавата, определяне на области за подобряване и изграждане на възможности за киберсигурност.

3.2 НИВА НА ЗРЯЛОСТ

Рамката се основава на **пет нива на зрялост**, определящи етапите, през които държавите членки преминават при изграждането на възможности за киберсигурност в областта, обхваната от всяка цел на НСКС. Нивата представляват нарастващи нива на зрялост, като се започне от първото **ниво 1** , при което държавите членки нямат ясно определен подход за изграждане на капацитет за киберсигурност в областите, обхванати от целите на НСКС, и се завърши с **ниво 5** , при което стратегията за изграждане на капацитет за киберсигурност е динамична и адаптивна към развитието на околната среда. Таблица 4 показва скалата за ниво на зрялост с описание на всяко ниво на зрялост.

Таблица 4: Скалата за зрялост от 5 нива на Националната рамка за оценка на възможностите на ENISA

НИВО 1 — НАЧАЛНО/AD HOC	НИВО 2 — РАННО ОПРЕДЕЛЯНЕ	НИВО 3 — СЪЗДАВАНЕ	НИВО 4 — ОПТИМИЗАЦИЯ	НИВО 5 — АДАПТИВНОСТ
Държавата членка няма ясно определен подход за изграждане на капацитет за киберсигурност в областите, обхванати от целите на НСКС. Въпреки това държавата може да има някои общи цели и да е извършила някои проучвания (технически, политически, политически, свързани с политиката) за подобряване на националните възможности.	Беше определен националният подход за изграждане на капацитет в областта, обхваната от целите на НСКС. Плановете за действие или дейностите за постигане на резултатите са налице, но на ранен етап. Освен това активните заинтересовани страни може да са били идентифицирани и/или ангажирани.	Планът за действие за изграждане на капацитет в областта, обхваната от целите на НСКС, е ясно определен и подкрепен от свързаните заинтересовани страни. Практиките и дейностите се прилагат и изпълняват еднакво на национално равнище. Дейностите са дефинирани и документирани с ясно разпределение на ресурсите и управление и набор от срокове.	Планът за действие се оценява редовно: подрежда се по приоритет, оптимизира се и е устойчив. Редовно се измерва изпълнението на дейностите по изграждане на капацитет за киберсигурност. Идентифицирани са факторите за успех, предизвикателства та и пропуските при изпълнението на дейностите.	Стратегията за изграждане на капацитет за киберсигурност е динамична и адаптивна. Постоянното внимание към развитието на околната среда (технологичен напредък, глобален конфликт, нови заплахи...) насърчава способността за бързо вземане на решения и способността да се действа бързо за подобряване.

3.3 КЛЪСТЕРИ И ОБШИРНА СТРУКТУРА НА РАМКАТА ЗА САМООЦЕНКА

Рамката за самооценка се характеризира с **четири клъстера**: (I) Управление и стандарти за киберсигурност, (II) изграждане на капацитет и осведоменост, (III) правни и регулаторни въпроси и (IV) сътрудничество. Всеки от тези клъстери обхваща ключова тематична област за изграждане на капацитет за киберсигурност в дадена държава и съдържа набор от различни цели, които държавите членки биха могли да включат в своята НСКС. По-конкретно:

- **(I) Управление и стандарти за киберсигурност**: този клъстер измерва капацитета на държавите членки да установят подходящо управление, стандарти и добри практики в областта на киберсигурността. Това измерение разглежда различни аспекти на киберотбраната и устойчивостта, като същевременно подкрепя развитието на националната промишленост за киберсигурност и изграждане на доверие в правителствата;
- **(II) Изграждане на капацитет и осведоменост**: този клъстер оценява капацитета на държавите членки да повишават осведомеността относно рисковете и заплахите за киберсигурността и начините за справяне с тях. В допълнение, това измерение измерва способността на държавата да изгражда непрекъснато възможности за киберсигурност и да повишава общото ниво на знания и умения в тази област. То разглежда развитието на пазара на киберсигурност и напредъка в научно - изследователската и развойна дейност в областта на киберсигурността. Този клъстер прегрупира всички цели, като полага основите за насърчаване на изграждането на капацитет;
- **(III) Правни и регулаторни въпроси**: този клъстер измерва капацитета на държавите членки да въведат необходимите правни и регулаторни инструменти за справяне и противодействие на увеличаването на киберпрестъпността и свързаните с нея киберинциденти, както и за защита на критичната

информационна инфраструктура. В допълнение, това измерение оценява и способността на държавите членки да създадат правна рамка за защита на гражданите и предприятията, както например в случай на балансиране на сигурността с личния живот; и

- **(IV) Сътрудничество:** този клъстер оценява сътрудничеството и обмена на информация между различните групи заинтересовани лица на национално и международно равнище като важен инструмент за по-добро разбиране и реагиране на постоянно променящата се застрашена среда.

Целите, които са включени в модела, са тези, които обикновено се приемат от държавите членки и са избрани от целите, изброени в раздел 2.2. По-специално, моделът оценява следните цели:

- 1. Разработване на национални планове за действие при извънредни ситуации, свързани с киберсигурността (I)
- 2. Установяване на базови мерки за сигурност (I)
- 3. Осигуряване на цифрова идентичност и изграждане на доверие в цифровите обществени услуги (I)
- 4. Създаване на възможности за реагиране при инциденти (II)
- 5. Повишаване на осведомеността на потребителите (II)
- 6. Организиране на дейности по киберсигурност (II)
- 7. Засилване на обучението и образователните програми (II)
- 8. Насърчаване на научно-изследователска и развойна дейност (II)
- 9. Осигуряване на стимули за частния сектор за инвестиции в мерки за сигурност (II)
- 10. Подобряване на киберсигурността на веригата за доставки (II)
- 11. Защита на критичната информационна инфраструктура, ООУ и доставчик на цифрови услуги (III)
- 12. Справяне с кибер престъпленията (III)
- 13. Създаване на механизми за докладване на инциденти (III)
- 14. Укрепване на неприкосновеността на личния живот и защитата на данните (III)
- 15. Институционализиране на сътрудничеството между публичните агенции (IV)
- 16. Участие в международно сътрудничество (IV)
- 17. Създаване на публично-частно партньорство (IV)

Четирите клъстера и основните цели се съчетават в модела за цялостен поглед върху зрелостта на възможностите за киберсигурност на държавите членки. Фигура 1 представя обширната структура на рамката за самооценка и показва как тези елементи, а именно, целите, клъстерите и рамката за самооценка, са свързани с оценката на изпълнението на дадена държава.

Фигура 1: Рамкова структура за самооценка

За всяка цел, включена в рамката за самооценка, съществуват редица показатели, разпределени между петте нива на зрялост. Всеки показател се основава на дихотомен въпрос (да/не). Показателят може да бъде задължителен или незадължителен.

3.4 МЕХАНИЗЪМ ЗА ОЦЕНЯВАНЕ

Механизмът за оценяване на рамката за самооценка взема предвид гореспоменатите елементи и принципите, изброени в раздел 3.5. В действителност, моделът осигурява оценка въз основа на стойността на два параметъра, **нивото на зрялост** и **коефициента на покритие**. Всеки от тези параметри може да бъде изчислен на различни нива: i) за цел, ii) на клъстер от цели или iii) като цяло.

Оценки на обективно ниво

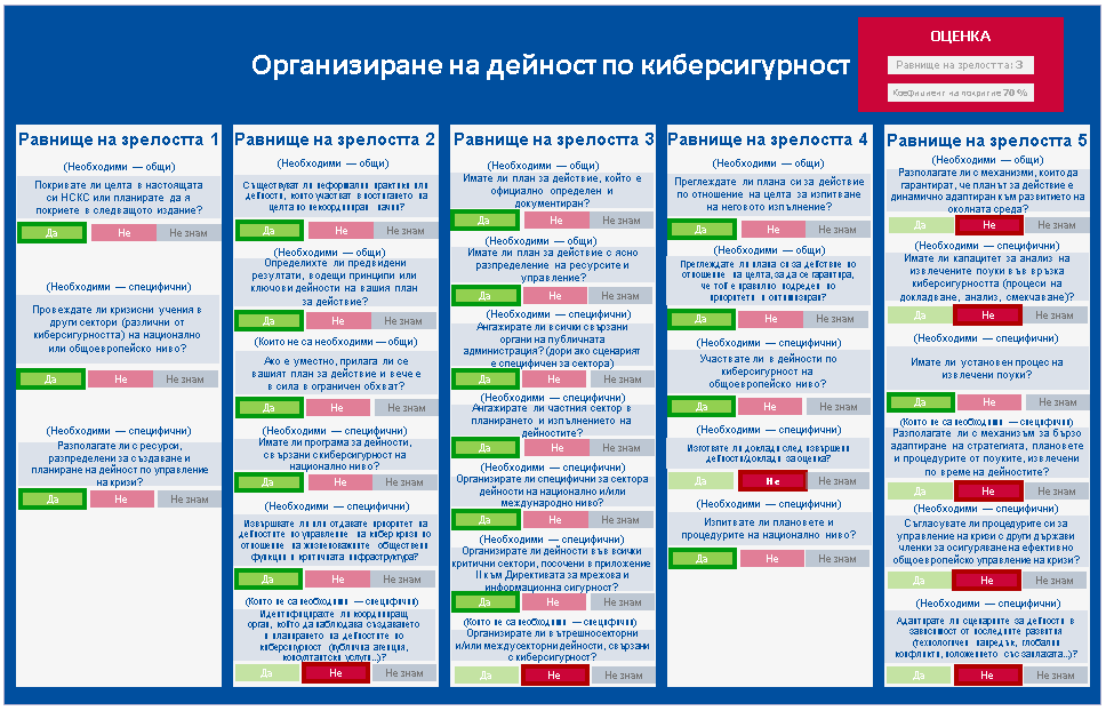
Оценката на нивото на зрялост дава преглед на нивото на зрялост, като показва какви възможности и практики са въведени. Оценката на нивото на зрялост се изчислява като най-високото ниво, за което респондентът отговаря на всички изисквания (*m.e.* отговор „Да“ на всички изисквани въпроси), освен че е изпълнил всички изисквания на предходните нива на зрялост.

Коефициентът на покритие показва степента на покритие на всички показатели, за които отговорът е положителен, независимо от тяхното ниво. Това е допълнителна стойност, която взема предвид всички показатели, измерващи дадена цел. Коефициентът на покритие се изчислява като съотношение между общия брой въпроси в рамките на целта и броя въпроси, за които отговорът е положителен.

Важно е да се изясни, че за останалата част от документа, думата ***„оценка“*** се използва за обозначаване както на стойностите на нивото на зрялост, така и на коефициента на покритие.

Фигура 2 — Механизмът за оценка за всяка цел осигурява визуализация на механизма за оценка, описан в раздел 3.1, който ще бъде доразвит по-долу.

Фигура 2: Механизъм за оценяване за цел



Фигура 2 показва пример за това как нивото на зрялост се изчислява за цел. Струва си да се отбележи, че респондентът е изпълнил всички изисквания на първите три нива на зрялост и е изпълнил само частично тези на ниво 4. Следователно оценката показва, че ***нивото на зрялост на респондента е ниво 3 за целта „Организиране на дейност по киберсигурност“*** *.*

Въпреки това, в примера, представен в Фигура 2, нивото на зрялост на целта не може да обхване информацията, предоставена от показателите, които имат положителна оценка и които са над ниво 3 на зрялост. В този случай коефициентът на покритие може да предостави преглед на всички елементи, които респондентът е изпълнил за постигането на тази цел, въпреки действителното му ниво на зрялост. В този случай съотношението между общия брой въпроси в рамките на целта и броя въпроси, за които отговорът е положителен, е равно на 19/27, т.е. стойността на ***коефициента на покритие е 70 %.***

Освен това, за да се адаптира към спецификата на държавите членки, като същевременно позволява последователен преглед, оценката се изчислява от две различни извадки на ниво клъстер и на общо ниво:

- **Общи оценки:** една пълна извадка, която обхваща всички цели, включени в клъстера или в общата рамка (от едно до 17);
- **Специфични оценки:** една специфична извадка, която обхваща само целите, избрани от държавата членка (обикновено съответстващи на целите, представени в НСКС на конкретната държава) в клъстера или в цялостната рамка.

Оценки на ниво клъстер

Общото ниво на зрялост на всеки клъстер се изчислява като средноаритметична стойност на нивото на зрялост на всички цели в този клъстер.

Специфичното ниво на зрялост на всеки клъстер се изчислява като средноаритметична стойност на нивото на зрялост на целите в рамките на този клъстер, която държавата членка е избрала да оцени (обикновено съответстваща на целите, представени в НСКС на конкретната държава).

Например, Фигура 1 показва, че клъстер (I) управление и стандарти за киберсигурност е съставен от три цели. Като се приема, че респондентът е избрал да оцени само първите две цели, но не и третата, и като се приема, че първите две цели представляват съответно ниво на зрялост от 2 и 4, тогава нивото на зрялост на клъстера, отчитайки всички цели, е ниво 2 (клъстер (I) общо ниво на зрялост = (2+ 4)/3), докато нивото на зрялост на клъстера, като се вземат предвид само конкретните цели, избрани от оценителя, е ниво 3 (клъстер (I) специфично ниво на зрялост = (2+ 4)/2).

Общият коефициент на покритие на всеки клъстер се изчислява като съотношението между общия брой въпроси в клъстера и броя въпроси, за които отговорът е положителен.

Коефициентът на специфично покритие на всеки клъстер се изчислява като съотношението между общия брой въпроси в клъстера, които се отнасят до целите, които държавата членка е избрала да оцени (обикновено съответстващо на целите, представени в НСКС на конкретната държава) и броя въпроси, за които отговорът е положителен.

Оценки на общо ниво

Общото ниво на зрялост на дадена държава се изчислява като средноаритметична стойност на нивото на зрялост на всички цели в рамката, от една до 17.

Общото специфично ниво на зрялост на държава се изчислява като средноаритметичната стойност на нивото на зрялост на целите в рамката, която държавата членка е избрала да оцени (обикновено съответстваща на целите, които присъстват в НСКС на конкретната държава).

Общият коефициент на общо покритие на дадена държава се изчислява като съотношението между общия брой въпроси във всички цели, включени в рамката (от една до 17) и броя въпроси, за които отговорът е положителен.

Общият коефициент на специфично покритие на дадена държава се изчислява като съотношението между общия брой въпроси в рамките на целите в рамката, което държавата членка е избрала да оцени (обикновено съответстващо на целите, представени в НСКС на конкретната държава) и броя въпроси, за които отговорът е положителен.

За всеки индикатор респондентите могат да изберат трета опция „не зная/неприложимо“ за своя отговор. В този случай показателят се изключва от общото изчисление на резултатите.

Нивата на зрялост на ниво клъстер и на общото ниво се изчисляват със средноаритметична стойност, за да се покаже напредъкът между две оценки. В действителност алтернативата, която се състои в изчисляването на клъстера и общите нива на зрялост като равнището за зрялост на най-незрялата цел — макар и от значение от гледна точка на зрелостта, не може да отчете напредъка, постигнат в области, обхванати от други цели.

Тъй като нивото на клъстера и общото ниво са консолидирани за целите на докладването, решено е да се използва средноаритметичната средна стойност. За по-голяма точност, моля използвайте оценките на обективно ниво за целите на докладването.

На фигура 3 по-долу са обобщени механизмите за оценяване на различните нива на модела (цел, клъстер, като цяло).

Фигура 3: Механизъм за обща оценка

3.5 ИЗИСКВАНИЯ КЪМ РАМКАТА ЗА САМООЦЕНКА

Националната рамка за оценка на възможностите, представена в настоящия раздел, се основава на потребностите, подчертани от държавите членки и е изградена върху набор от изисквания, изброени по-долу:

- НРОВ се въвежда доброволно от държавата членка като рамка за самооценка;
- НРОВ има за цел да измери възможностите за киберсигурност на държавите членки по отношение на 17-те цели. Въпреки това държавата членка може да избере целите, които желае да оцени, и да оценява само подмножество от 17-те цели;
- Рамката за самооценка има за цел да измери степента на зрялост на възможностите за киберсигурност на държавата членка;
- Резултатите от оценката не се публикуват, освен ако държавата членка не реши да направи това по своя собствена инициатива;

- Държавата членка може да покаже резултатите от оценката чрез представяне на нивото на зрялост на възможностите за киберсигурност на държавата, на клъстер от цели или дори на една единствена цел;
- Всички оценени цели са еднакво релевантни в рамката за оценка, следователно те имат еднакво значение. Същото се прилага и за показателите, разположени в нея; и
- Държавата членка може да следи напредъка си с течение на времето.

Рамката за самооценка има за цел да подпомогне държавите членки в изграждането на възможности за киберсигурност, следователно тя включва и набор от препоръки или насоки за насочване на европейските държави в подобряването на тяхното ниво на зрялост.

Бележка: тези препоръки или насоки са общи и основани на публикациите на ENISA и извлечените поуки от други държави; те ще зависят резултата от самооценката.

4. ПОКАЗАТЕЛИ НА НРОВ

4.1 РАМКОВИ ПОКАЗАТЕЛИ

Този раздел представя показателите на националната рамка за оценка на възможностите на ENISA. Следните раздели са организирани по клъстер.

За всеки клъстер в таблица е представен цялостния набор от показатели под формата на въпроси, представителни за определено ниво на зрялост. Въпросникът е основният инструмент за самооценка. За всяка цел има два набора от показатели, които трябва да бъдат отбелязани:

- Набор от общи въпроси за зрялост на стратегията (9 общи въпроси), маркирани от „а“ до „в“ за всяко ниво на зрялост, повторено за всяка цел; и
- Набор от въпроси за капацитета за киберсигурност (319 въпроса за капацитета за киберсигурност), номерирани от „1“ до „10“ за всяко ниво на зрялост, специфично за областта, обхваната от целта.

Всеки въпрос е представен с таг (0—1), който посочва дали въпросът е задължителен показател (1) или незадължителен показател (0) за нивото на зрялост.

Всеки въпрос може да бъде идентифициран с идентификационен номер, състоящ се от:

- Обективния номер;
- Нивото на зрялост; и
- Номерът на въпроса.

Например, въпрос ID 1.2.4 е четвъртият въпрос в ниво на зрялост 2 на стратегическата цел (I) „Разработване на национални планове за действие при извънредни ситуации, свързани с киберсигурността“.

Трябва да се отбележи, че в целия въпросник обхватът на въпросите е на национално равнище, освен ако не е посочено друго. Във всички въпроси местоимението „Вие“ се отнася до държавата членка по общ начин и не се отнася до отделния или държавен орган, който извършва оценката.

Определението на всяка цел може да бъде намерено в глава 2.2 - Общи цели, определени в рамките на Европейската НСКС.

4.1.1 Клъстер #1: Управление и стандарти за киберсигурност

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
1 – Разработване на национални планове за действие при извънредни ситуации, свързани с киберсигурността	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Започнахте ли да работите по изграждането на национални планове за действие при извънредни ситуации, свързани с киберсигурността? *Напр.* определяне на общите цели, обхват и/или принципи на плановете за действие при извънредни ситуации...	1	Имате ли доктрина/национална стратегия, която включва киберсигурността като кризисен фактор (т.е. план, политика и т.н.)?	1	Имате ли план за управление на кибер кризи на национално ниво?	1	Доволни ли сте от броя или процента на критичните сектори, включени в националния план за действие при извънредни ситуации, свързани с киберсигурността?	1	Имате ли процес на „учене на уроци“ след свързани с киберсигурност дейности или действителни кризи на национално равнище?	1
	2	Разбира ли се, че киберинцидентите представляват кризисен фактор, който може да застраши националната сигурност?	0	Имате ли център за получаване на информация и информиране на лицата, вземащи решения? *Т.е.* каквито и да е методи, платформи или местоположения, за да се гарантира, че всички участници в кризисни ситуации могат да получат достъп до една и съща информация в реално време за киберкризата.	1	Разполагате ли с процедури за кибер криза на национално ниво?	1	Организирате ли достатъчно често дейности (т.е. инициативи), свързани с националното планиране за действие при извънредни ситуации, свързани с киберсигурността?	1	Разполагате ли с процес за редовно изпитване на националния план?	1
	3	Проведени ли са проучвания (технически, оперативни, политически) в областта на планирането за действие при извънредни ситуации, свързани с киберсигурността?	0	Ангажирани ли са съответните ресурси за наблюдение на разработването и изпълнението на националните планове за действие при извънредни ситуации, свързани с киберсигурността?	1	Разполагате ли с екип за комуникация, специално обучен да реагира на кибер кризи и да информира обществеността?	1	Разполагате ли с достатъчно хора, посветени на планирането на кризи, разглеждането на извлечените поуки и осъществяването на промяна?	1	Разполагате ли с адекватни инструменти и платформи за изграждане на информираност за ситуацията?	1

	4	-		Разполагате ли с методика за оценка на кибер заплахата на национално равнище, която включва процедури за оценка на въздействието?	0	Ангажирате ли всички съответни национални заинтересовани страни (национална сигурност, отбрана, гражданска защита, правоприлагане, министерства, органи и др.?)	1	Разполагате ли с достатъчно хора, обучени да реагират на кибер кризи на национално ниво?	1	Следвате ли конкретен модел за зрялост за наблюдение и подобряване на плана за действие при извънредни ситуации, свързани с киберсигурността?	0
	5	-		-		Разполагате ли с подходящи съоръжения за управление на кризи и ситуационни зали?	1	-		Разполагате ли с ресурси, специализирани в прогнозиране на заплахи или работа по бъдещи въпроси, свързани с киберсигурността за справяне с бъдеща криза или утрешни предизвикателства?	0
	6	-		-		Работите ли с международни заинтересовани страни в ЕС, ако е необходимо?	0	-		-	
	7	-		-		Работите ли с международни заинтересовани страни в държави извън ЕС, ако е необходимо?	0	-		-	
Цел на НСКС	**#**	**Ниво 1**	**С**	**Ниво 2**	**С**	**Ниво 3**	**С**	**Ниво 4**	**С**	**Ниво 5**	**С**
2 – Установяване на базови мерки за сигурност	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Извършвали ли сте проучване за идентифициране на изискванията и пропуските за **публичните** организации въз основа на международно признати стандарти? *Напр.* ISO27001 , ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, IEC, CIS...	1	Предприети ли са мерките за сигурност в съответствие с международните/националните стандарти?	1	Задължителни ли са базовите мерки за сигурност?	1	Съществува ли процес за често актуализиране на базовите мерки за сигурност?	1	Имате ли процес за подсилване на ИКТ, когато мерките не успяват да разрешат инцидентите?	1

	2	Извършвали ли сте проучване за идентифициране на изискванията и пропуските за **частните** организации въз основа на международно признати стандарти? Напр. ISO27001 , ISO27002, BS 15000, EN ISO27799, PCI-DSS, CobiT, ITIL, BSI IT-Grundschutz, IETF, IEEE, NIST, FIPS, ITU, IEC, CIS...	1	Допитват ли се до частния сектор и други заинтересовани страни при определянето на базовите мерки за сигурност?	1	Прилагате ли хоризонтални мерки за сигурност в критични сектори?	1	Съществува ли механизъм за наблюдение за проучване на усвояването на базовите мерки за сигурност?	1	Оценявате ли значението на новите стандарти, които са разработени в отговор на най-новото развитие на положението със заплахата?	1
	3	-		-		Прилагате ли специфични за сектора мерки за сигурност в рамките на критични сектори?	1	Съществува ли национален орган, който да проверява дали базовите мерки за сигурност се прилагат или не?	1	Разполагате ли или насърчавате ли национален координиран процес за разкриване на уязвимостта (CVD)?	1
	4	-				Съответстват ли базовите мерки за сигурност на съответните схеми за сертифициране?	1	Разполагате ли с процес за идентифициране на неспазващи организации в рамките на определен период от време?	1	-	
	5	-		-		Съществува ли процес на самооценка на риска за базовите мерки за сигурност?	1	Съществува ли процес на одит, който да гарантира, че мерките за сигурност се прилагат правилно?	1	-	
Цел на НСКС	**#**	**Ниво 1**	**С**	**Ниво 2**	**С**	**Ниво 3**	**С**	**Ниво 4**	**С**	**Ниво 5**	**R**
2 – Установяване на базови мерки за сигурност	6	-		-		Преглеждате ли задължителните базови мерки за сигурност в процеса на възлагане на обществени поръчки на правителствени органи?	0	Определяте ли или активно насърчавате приемането на сигурни стандарти за разработването на критични ИТ/ОТ продукти (медицинско оборудване, свързани и автономни превозни средства, професионално радио, тежко индустриално оборудване...)?	0	-	

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
3 – Осигуряване на цифрова идентичност и изграждане на доверие в цифровите обществени услуги	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Извършвали ли сте проучвания или анализи на пропуските, за да установите необходимостта от осигуряване на цифрови обществени услуги за гражданите и предприятията?	1	Извършвате ли анализи на риска за определяне на рисковия профил на активите или услугите, преди да ги преместите в облака или да ангажирате каквито и да е проекти за цифрова трансформация?	1	Насърчавате ли методологиите за „защитата на личните данни още при проектирането“ във всички проекти за електронно управление?	1	Събирате ли показатели за инциденти, свързани с киберсигурността, които касаят нарушаването на цифровите обществени услуги?	1	Участвате ли в европейски работни групи за поддържане на стандарти и/или създаване на нови изисквания за електронни доверителни услуги (електронни подписи, електронни печати, електронни регистрирани услуги за доставка, електронен времеви печат, идентификация на уебсайта)? *Напр.* ETSI /CEN/CENELEC, ISO, IETF, NIST, ITU...	1
	2	-		Имате ли стратегия за изграждане или насърчаване на сигурни национални схеми за електронна идентификация за гражданите и предприятията?	1	Включвате ли частни заинтересовани страни в създаването и предоставянето на сигурни цифрови обществени услуги?	1	Прилагали ли сте взаимно признаване на средствата за електронна идентификация с други държави членки?	1	Участвате ли активно в партньорските проверки като част от нотифицирането на схемите за електронна идентификация до Европейската комисия?	1
	3	-		Имате ли стратегия за изграждане или насърчаване на сигурни национални електронни доверителни услуги (електронни подписи, електронни печати, електронни регистрирани услуги за доставка, електронен времеви печат, идентификация на уебсайта) за гражданите и предприятията?	1	Прилагате ли минимална базова линия за сигурност за всички цифрови обществени услуги?	1	-		-	

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
3 – Осигуряване на цифрова идентичност и изграждане на доверие в цифровите обществени услуги	4	-		Имате ли стратегия за правителствения облак (облачна изчислителна стратегия, насочена към правителството и публичните органи, като министерствата, правителствени агенции и публични администрации...), която отчита последиците за сигурността?	0	Разполагате ли с електронни схеми за идентификация на гражданите и предприятията със значително или високо ниво на сигурност, както е определено в приложението към Регламент (ЕС) № 910/2014 относно електронната идентификация?	1	-		-	
	5	-		-		Разполагате ли с цифрови обществени услуги, които изискват схеми за електронна идентификация със значително или високо ниво на сигурност, както е определено в приложението към Регламент (ЕС) № 910/2014 относно електронната идентификация?	1	-		-	
	6	-		-		Имате ли доставчици на доверителни услуги за гражданите и бизнеса (електронни подписи, електронни печати, електронни регистрирани услуги за доставка, електронен времеви печат, идентификация на уебсайта)?	1	-		-	
	7	-		-		Насърчавате ли приемането на базовите мерки за сигурност за всички модели за разгръщане на облака (напр. частни, публични, хибридни. инфраструктура като услуга, платформа като услуга, софтуер като услуга)?	0	-		-	

4.1.2 Клъстер #2: Изграждане на капацитет и осведоменост

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
4 – Създаване на възможности за реагиране при инциденти	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Имате ли неформални възможности за реагиране на инциденти, управлявани в рамките или между публичния и частния сектор?	1	Имате ли поне един официален национален ЕРИКС?	1	Имате ли възможности за реагиране на инциденти за секторите, посочени в приложение II към Директивата за мрежова и информационна сигурност?	1	Определихте ли и насърчавахте ли стандартизирани практики за процедури за реагиране на инциденти и схемите за класификация на инциденти?	1	Имате ли механизми за ранно откриване, идентификация, превенция, отговор и смекчаване на уязвимостта на нулевия ден?	1
	2	-		Имат ли вашите национални ЕРИКС ясно определен обхват на намеса? *напр.* в зависимост от целевия сектор, видовете инциденти, въздействията	1	Наличен ли е механизъм за сътрудничество за ЕРИКС във вашата държава за отговор на инциденти?	1	Оценявате ли способността си за реагиране на инциденти за гарантиране, че разполагате с необходимите ресурси и умения за изпълнение на задачите, посочени в точка 2 от приложение I към Директивата за мрежова и информационна сигурност?	1	-	

	3	-		Дали вашите национални ЕРИКС имат ясно определени отношения с други национални заинтересовани страни по отношение на ситуацията с националната киберсигурност и практиката за реагиране на инциденти (напр. ПО, военни, интернет доставчици, НСКС)?	0	Вашите национални ЕРИКС разполагат с възможност за реагиране на инциденти в съответствие с приложение I към Директивата за мрежова и информационна сигурност? *m.e.* наличност , физическа сигурност, непрекъснатост на дейността, международно сътрудничество, мониторинг на инциденти, капацитет за ранно предупреждение и сигнали, реагиране на инциденти, анализ на риска и информираност за ситуацията, сътрудничество с частния сектор, стандартни практики...	1	-		-	
	4	-				Съществува ли механизъм за сътрудничество с други съседни държави във връзка с инцидентите?	1	-		-	
	5	-		-		Определихте ли официално ясни политики и процедури за справяне с инциденти?	1	-		-	
Цел на НСКС	**#**	**Ниво 1**	**С**	**Ниво 2**	**С**	**Ниво 3**	**С**	**Ниво 4**	**С**	**Ниво 5**	**С**
4 – Създаване на възможности за реагиране при инциденти	6	-		-		Дали вашите национални ЕРИКС участват в дейности по киберсигурност както на национално, така и на международно ниво?	1	-		-	
	7	-		-		Свързани ли са вашите национални ЕРИКС с FIRST (Форум за реагиране на инциденти и екипи за сигурност)?	0	-		-	

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
5 – Повишаване на осведомеността на потребителите	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Съществува ли минимално признание от страна на правителството, частния сектор или общите потребители, че е необходимо да се повиши осведомеността по въпросите на киберсигурността и неприкосновеността на личния живот?	1	Идентифицирали ли сте конкретна целева аудитория за информиране на потребителите? *Напр.* общи потребители, млади хора, бизнес потребители (които могат да бъдат разбити допълнително: МСП, ООУ, доставчици на цифрови услуги (ДЦУ) и др.)	1	Разработихте ли комуникационни планове/стратегия за кампаниите?	1	Изготвяте ли показатели за оценка на вашата кампания по време на етапа на планиране?	1	Разполагате ли с механизми за гарантиране, че кампаниите за информиране са постоянно приложими по отношение на технологичния напредък, промените в положението със заплахата, законовите разпоредби и директивите за национална сигурност?	1
	2	Публичните агенции провеждат ли кампании за информиране във връзка с киберсигурността в рамките на своята организация в конкретен случай? Напр. след инцидент, свързан с киберсигурността.	0	Изготвяте ли план на проекта за повишаване на осведомеността по въпросите на сигурността на информацията и неприкосновеността на личния живот?	1	Имате ли процес за създаване на съдържание на правителствено ниво?	1	Оценявате ли кампаниите си след изпълнение?	1	Извършвате ли периодична оценка или проучване за измерване на промяната в отношението или промените в поведението по отношение на киберсигурността и неприкосновеността на личния живот в частния и публичния сектор?	1

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
5 – Повишаване на осведомеността на потребителите	3	Публичните агенции провеждат ли кампании за осведоменост по отношение на киберсигурността пред широката общественост в конкретен случай? *Например* в следствие на инцидент с киберсигурност.	0	Имате ли налични ресурси и лесно разпознаваеми (*например* един онлайн портал, комплекти за осведоменост) за всички потребители, които се стремят да се образоват по въпросите на киберсигурността и неприкосновеността на личния живот?	1	Разполагате ли с каквито и да е механизми за идентифициране на целеви области за повишаване на осведомеността (т.е. положението във връзка със заплахата на ENISA, положение на държавата, международно положение, обратна връзка от националните центрове за борба с киберпрестъпността и т.н.)?	1	Разполагате ли с механизми за идентифициране на най-подходящия медиен или комуникационен канал в зависимост от целевата аудитория за увеличаване на достъпа и ангажираността? *Напр.* различни видове цифрови медии, брошури, имейли, учебни материали, плакати в натоварени области, телевизия, радио...	1	Консултирате ли се с поведенчески експерти, за да настроите кампанията си към целевата аудитория?	1
	4	-		-		Събирате ли заинтересованите страни с експерти и комуникационни екипи за създаване на съдържание?	1			-	
	5	-		-		Включвате ли и ангажирате ли частния сектор в усилията си за информиране за насърчаване и разпространяване на посланията до по-широка аудитория?	1	-		-	
	6	-		-		Подготвяте ли конкретни инициативи за информиране на ръководителите в публичния, частния, академичния сектор или гражданското общество?	1	-		-	
	7	-		-		Участвате ли в кампаниите на Европейския месец на киберсигурността (ЕМКС) на ENISA?	0	-		-	

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
6 – Организиране на дейности по киберсигурност	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		

6 – Организиране на дейности по киберсигурност	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0							
	1	Провеждате ли кризисни учения в други сектори (различни от киберсигурността) на национално или общоевропейско ниво?	1	Имате ли програма за дейности, свързани с киберсигурност на национално ниво?	1	Ангажирате ли всички свързани органи на публичната администрация? (дори ако сценарият е специфичен за сектора)	1	Пишете ли след доклади за действия/оценки?	1	Имате ли капацитет за анализ на извлечените поуки във връзка киберсигурността (процеси на докладване, анализ, смекчаване)?	1
	2	Разполагате ли с ресурси, разпределени за създаване и планиране на дейност по управление на кризи?	1	Извършвате ли или отдавате приоритет на дейностите по управление на кибер кризи по отношение на жизненоважните обществени функции и критичната инфраструктура?	1	Ангажирате ли частния сектор в планирането и изпълнението на дейностите?	1	Изпитвате ли плановете и процедурите на национално ниво?	1	Имате ли установен процес на извлечени поуки?	1
	3	-		Идентифицирахте ли координиращ орган, който да наблюдава създаването и планирането на дейностите по киберсигурност (публична агенция, консултантски услуги...)?	0	Организирате ли специфични за сектора дейности на национално и/или международно ниво?	1	Участвате ли в дейности по киберсигурност на общоевропейско равнище?	1	Адаптирате ли сценариите за дейности в зависимост от последните развития (технологичен напредък, глобални конфликти, положението със заплахата...)?	1
	4	-		-		Организирате ли дейности във всички критични сектори, посочени в приложение II към Директивата за мрежова и информационна сигурност?	1	-		Съгласувате ли процедурите си за управление на кризи с други държави членки за осигуряване на ефективно общоевропейско управление на кризи?	1
	5	-		-		Организирате ли вътрешносекторни и/или междусекторни дейности, свързани с киберсигурност?	1	-		Разполагате ли с механизъм за бързо адаптиране на стратегията, плановете и процедурите от поуките, извлечени по време на дейностите?	0
	6	-		-		Организирате ли дейности по киберсигурност, специфични за различните нива? (техническо и оперативно ниво, процедурно ниво, ниво на вземане на решения, политическо ниво...)	0	-		-	

Цел на НСКС	#	Level 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
7 – Засилване на обучението и образователните програми	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Обмисляте ли разработването на обучения и образователни програми по киберсигурност?	1	Провеждате ли курсове, посветени на киберсигурността?	1	Вашата държава възприела ли е културата на киберсигурността на ранния етап от обучението на учениците? Например, предпочитате ли киберсигурността в средното училище и гимназията?	1	Настоявате ли персоналът в частния и публичния сектор да бъде акредитиран или сертифициран?	1	Разполагате ли с механизми, които да гарантират, че обученията и образователните програми са постоянно приложими по отношение на настоящите и нововъзникващите технологични развития, промените в положението във връзка със заплахата, законовите разпоредби и директивите за националната сигурност?	1
	2	-		Дали университетите от вашата държава предлагат докторантури по киберсигурност като независима дисциплина, а не в рамките на предмета „компютърни науки“?	1	Имате ли национални изследователски лаборатории и образователни институции, които са специализирани в киберсигурността?	1	Разработила ли е вашата държава програми за обучение по киберсигурност или менторство в подкрепа на националните стартиращи предприятия и МСП?	1	Създавате ли академични центрове за високи постижения в киберсигурността, за да действате като центрове за научни изследвания и образование?	1
	3	-		Планирате ли да обучите преподаватели, независимо от тяхната област, по въпросите на информационната сигурност и неприкосновеността на личния живот? *Напр.* онлайн безопасност, защита на личните данни, кибер тормоз.	1	Насърчавате ли/финансирате ли специализирани курсове по киберсигурност и планове за обучение на служители на агенциите по заетостта на държавите членки?	1	Активно ли насърчавате добавянето на курсове за информационна сигурност във висшето образование не само за студенти по компютърни науки, но и към всяка друга професионална специалност? *напр.* курсове, съобразени с нуждите на тази професия.	1	Участват ли академичните институции във водещи дискусии в областта на образованието и научните изследвания за киберсигурност в международен план?	0

	4	-		-		Имате ли курсове за киберсигурност и/или специализирана учебна програма за ЕКР (Европейска квалификационна рамка) на ниво 5 — 8?	1	Оценявате ли редовно липсата на умения (недостиг на работници в киберсигурността) в областта на информационната сигурност?	1	-	
	5	-		-		Насърчавате ли и/или подкрепяте инициативи за включване на курсовете за безопасност в Интернет в основното и средното образование?	1	Насърчавате ли споделянето в мрежа и обмена на информация между академичните институции както на национално, така и на международно ниво?	1		
Цел на НСКС	**#**	**Ниво 1**	**С**	**Ниво 2**	**С**	**Ниво 3**	**С**	**Ниво 4**	**С**	**Ниво 5**	**С**
7 - Засилване на обучението и образователните програми	6	-		-		Финансирате ли или предлагате безплатни основни обучения по киберсигурност на гражданите?	0	Включвате ли частния сектор в каквато и да е форма в образователни инициативи за киберсигурност? *Напр.* създаване и провеждане на курсове, стажове, работни места...	1	-	
	7	-		-		Организирате ли годишни събития за информационна сигурност (напр. хакерски конкурси или хекатони)?	0	Прилагате ли механизми за финансиране с цел насърчаване на усвояването на степени на киберсигурност? *Напр.* стипендии , гарантирано чиракуване/стаж, гарантирани работни места в конкретна промишленост или роли в публичния сектор	0	-	

Цел на НСКС	**#**	**Ниво 1**	**С**	**Ниво 2**	**С**	**Ниво 3**	**С**	**Ниво 4**	**С**	**Ниво 5**	**С**
8 – Насърчаване на научно-изследователска и развойна дейност	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						

	1	Извършвали ли сте проучвания или анализи за идентифициране на приоритетите на научно - изследователската и развойна дейност за киберсигурност?	1	Имате ли процес за определяне на приоритети на научно - изследователската и развойна дейност (например възникващи теми за възпиране, защита, откриване и адаптиране към нови видове кибератаки)?	1	Съществува ли план за свързване на инициативите за научно - изследователска и развойна дейност с реалната икономика?	1	Дали инициативите, свързани с научно - изследователската и развойна дейност за киберсигурност са в съответствие със съответните стратегически цели, например ЦЕП, „Хоризонт 2020“, програма „Цифрова Европа“, стратегия на ЕС за киберсигурност?	1	Осъществявате ли сътрудничество на национално ниво с международни инициативи, свързани с научно - изследователска и развойна дейност за киберсигурност?	1
	2	-		Участва ли частният сектор в създаването на приоритети за научно - изследователска и развойна дейност?	1	Съществуват ли национални проекти, свързани с киберсигурността?	1	Съществува ли схема за оценка на инициативите за научно - изследователска и развойна дейност?	1	Приоритетите, свързани с научно - изследователска и развойна дейност съобразени ли са с настоящия или предстоящ регламент (национално ниво)?	1
Цел на НСКС	**#**	**Ниво 1**	**С**	**Ниво 2**	**С**	**Ниво 3**	**С**	**Ниво 4**	**С**	**Ниво 5**	**С**
8 – Насърчаване на научно-изследователска и развойна дейност	3	-		Академичните среди участват в създаването на приоритети за научно-изследователска и развойна дейност?	1	Имате ли местни/регионални стартиращи екосистеми и други мрежови канали (например технологични паркове, иновационни клъстери, събития в мрежа/платформи) за насърчаване на иновациите (включително за стартиращи компании в сферата на киберсигурността)?	1	Съществуват ли споразумения за сътрудничество с университети и други изследователски институти?	1	Участвате ли във водещи дискусии в една или много авангардни теми за научно - изследователска и развойна дейност на международно ниво?	0
	4	-		Съществуват ли национални инициативи за научно-изследователска и развойна дейност, свързани с киберсигурността?	0	Има ли инвестиции в програми, свързани с научно - изследователска и развойна дейност за киберсигурност в академичните среди и частния сектор?	1	Има ли признат институционален орган, който наблюдава дейности, свързани с научно - изследователска и развойна дейност за киберсигурност?	0	-	
	5	-		-		Имате ли позиции за индустриални изследвания в университетите, които да свържат научните изследвания и нуждите на пазара?	1	-		-	
	6	-		-		Имате ли определени програми за финансиране на научно - изследователска и развойна дейност за киберсигурност?	0	-		-	

Цел на НСКС	#	Level 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
9 — Осигуряване на стимули за частния сектор за инвестиции в мерки за сигурност	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Съществува ли промишлена политика или политическа воля за насърчаване на развитието на индустрията за киберсигурност?	1	Частният сектор участва ли в създаването на стимули?	1	Съществуват ли икономически/регулаторни или други видове стимули за насърчаване на инвестициите в киберсигурност?	1	Има ли частни участници, които реагират на стимули, като инвестират в мерки за сигурност ? *Напр.* инвеститори, специализирани в киберсигурност и неспециализирани инвеститори	1	Насочвате ли стимулите върху темите на киберсигурността в зависимост от последните развития, свързани със заплахата?	1
Цел на НСКС	**#**	**Ниво 1**	**С**	**Ниво 2**	**С**	**Ниво 3**	**С**	**Ниво 4**	**С**	**Ниво 5**	**С**
9 — Осигуряване на стимули за частния сектор за инвестиции в мерки за сигурност	2	-		Идентифицирахте ли конкретни теми за киберсигурност, които да бъдат разработени? *Напр.* криптография , неприкосновеност на личния живот, нова форма на автентикация, изкуствен интелект за киберсигурност...	0	Предоставяте ли подкрепа (напр. данъчни стимули) за стартиращи компании в сферата на киберсигурността и МСП?	1	Предоставяте ли стимули за частния сектор да наблегне на сигурността на авангардните технологии? *Напр.* 5G , изкуствен интелект, интернет на предметите, квантови изчисления...	1	-	
	3	-		-		Предоставяте ли данъчни стимули или друга финансова мотивация за инвеститорите от частния сектор в стартиращи компании в сферата на киберсигурността?	1	-		-	
	4	-		-		Улеснявате ли достъпа на свързани с киберсигурността стартиращи компании и МСП в процеса на възлагане на обществени поръчки?	0	-		-	
	5	-		-		Има ли бюджет за предоставяне на стимули за частния сектор?	0	-		-	

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
10 – Подобряване на киберсигурността на веригата за доставки	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Извършвали ли сте проучване на добрите практики за сигурност за управление на веригата за доставки, използвана от обществените поръчки в различни промишлени сегменти и/или в публичния сектор?	1	Извършвате ли оценки на киберсигурността по цялата верига за доставки на ИКТ услуги и продукти в критични сектори (както е посочено в приложение II към Директива (ЕС) 2016/1148 за мрежова и информационна сигурност?	1	Използвате ли схема за сертифициране на сигурността за продукти и услуги, разработени на базата на ИКТ? *Напр.* ГСС на SOG-IS в Европа (Група на старши служители за сигурност на информационните системи, споразумение за взаимно признаване), Споразумение за признаване на общи критерии (СПОК), национални инициативи, секторни инициативи...	1	Разполагате ли с процес за актуализиране на оценките на киберсигурността на веригата за доставки на ИКТ услуги и продукти в критични сектори (както е посочено в приложение II към Директива (ЕС) 2016/1148 за мрежова и информационна сигурност?	1	Разполагате ли със сонди за откриване в ключови елементи във веригата за доставки за откриване на ранен признак на компромис? *Напр.* контроли за сигурност на ниво ISP, сонди за сигурност в основните компоненти на инфраструктурата...	1

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
10 – Подобряване на киберсигурността на веригата за доставки	2	-		Прилагате ли стандарти в политиките за възлагане на обществени поръчки на публичните администрации за гарантиране, че доставчиците на ИКТ продукти или услуги отговарят на основните изисквания за информационна сигурност? *Напр.* ISO/IEC 27001 и 27002, ISO/IEC 27036...	1	Активно ли насърчавате сигурността и неприкосновеността на личния живот чрез създаване на най-добри практики при разработването на ИКТ продукти и услуги? *Напр.* сигурен жизнен цикъл на разработка на софтуер, жизнен цикъл на интернет на предметите	1	Разполагате ли с процес за идентифициране на слабите връзки в киберсигурността във веригата за доставки на критичните сектори (както е посочено в приложение II към Директива (ЕС) 2016/1148 за мрежова и информационна сигурност?	1	-	
	3	-		-		Разработвате и предоставяте ли централизирани каталози с разширена информация за съществуващите стандарти за информационна сигурност и неприкосновеност на личния живот, които са мащабируеми и приложими от МСП?	1	Разполагате ли с механизми, които да гарантират, че ИКТ продуктите и услугите, които са от решаващо значение за ООУ, са киберустойчиви (*т.е.* способността да се поддържа наличността и безопасността срещу кибер инциденти)? *Напр.* чрез изпитване, редовни оценки, откриване на компрометирани елементи...	1	-	
	4	-				Участвате ли активно в създаването на рамка на ЕС за сертифициране на ИКТ цифрови продукти, услуги и процеси, както е посочено в Акта за киберсигурността на ЕС (Регламент (ЕС) 2019/881)? *Напр.* участие в Европейската група за сертифициране на киберсигурността (ЕГСКС), насърчаване на техническите стандарти и процедури за сигурността на ИКТ продукти/услуги	0	Насърчавате ли разработването на схеми за сертифициране, насочени към МСП, за повишаване на сигурността на информацията и приемането на стандарта за неприкосновеност на личния живот?	0	-	
	5	-		-		Предоставяте ли някакви видове стимули на МСП да приемат стандарти за сигурност и неприкосновеност на личния живот?	0	Имате ли разпоредби, които да насърчат големите дружества да увеличат киберсигурността на малките предприятия във веригите си за доставки? *Напр.* център за киберсигурност, кампании за обучение и информираност...	0	-	

	6	-		-		Насърчавате ли доставчиците на софтуер да подкрепят МСП, като гарантират сигурни конфигурации по подразбиране в продукти, насочени към малки организации?	0	-		-

4.1.3 Клъстер #3: Правни и регулаторни въпроси

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
11 – Защита на критичната информационна инфраструктура, ООУ и доставчик на цифрови услуги	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Съществува ли общо разбиране, че операторите на критична информационна инфраструктура допринасят за националната сигурност?	1	Имате ли методология за идентифициране на основни услуги?	1	Приложихте ли Директива (ЕС) 2016/1148 за мрежова и информационна сигурност?	1	Имате ли процедура за актуализиране на регистъра на риска?	1	Създавате ли и актуализирате ли доклади за положението във връзка със заплахата?	1
	2	-		Имате ли методология за идентифициране на критична информационна инфраструктура?	1	Приложихте ли Директивата 2008/114/ЕО относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита?	1	Разполагате ли с други механизми за измерване, че техническите и организационните мерки, предприети от ООУ, са подходящи за управлението на рисковете, свързани със сигурността на мрежовите и информационните системи? Напр. редовни проверки на киберсигурността, национална рамка за прилагането на стандартни мерки, технически инструменти, предоставени от правителството като сонди за откриване или специфичен за системата преглед на конфигурацията...	1	В зависимост от последните развития на положението със заплахата, можете ли да приемете нов сектор във вашия план за действие за защита на критичната информационна инфраструктура?	1
	3	-		Имате ли методология за идентифициране на ООУ?	1	Имате ли национален регистър за идентифициран ООУ за критичен сектор?	1	Преглеждате ли и съответно актуализирате списъка на идентифицираните ООУ най-малко на всеки две години?	1	В зависимост от последните развития на положението със заплахата, можете ли да адаптирате нови изисквания във вашия план за действие за защита на критичната информационна инфраструктура?	1

Цел на НСКС	#										
11 – Защита на критичната информационна инфраструктура, ООУ и доставчик на цифрови услуги	4	-		Имате ли методология за идентифициране на доставчиците на цифрови услуги?	1	Имате ли национален регистър за идентифицирани доставчици на цифрови услуги?	1	Разполагате ли с други механизми за измерване, че техническите и организационните мерки, приложени от доставчиците на цифрови услуги, са подходящи за управлението на рисковете, свързани със сигурността на мрежовите и информационните системи? Напр. редовни проверки на киберсигурността, национална рамка за прилагането на стандартни мерки, технически инструменти, предоставени от правителството като сонди за откриване или специфичен за системата преглед на конфигурациите ...	1	-	
	5	-		Разполагате ли с един или повече национални органи, които осигуряват надзор върху защитата на критичната информационна инфраструктура и сигурността на мрежовите и информационните системи? Напр. според изискванията на Директива (ЕС) 2016/1148 за мрежова и информационна сигурност	1	Имате ли национален регистър на риска за идентифицирани или известни рискове?	1	Преглеждате ли и съответно актуализирате списъка на идентифицираните доставчици на цифрови услуги най-малко на всеки две години?	1	-	
	6	-		Разработвате ли специфични за сектора планове за защита? Напр. включително базовите мерки за киберсигурност (задължителни или насоки)	0	Имате ли методология за картографиране на зависимостите от критична информационна инфраструктура?	1	Използвате ли схема за сертифициране на сигурността (национална или международна), за да помогнете на ООУ и доставчиците на цифрови услуги да идентифицират сигурни ИКТ продукти? Напр. СВП на SOG-IS в Европа, национални инициативи...	1	-	

	7	-		-		Прилагате ли практики за управление на риска за определяне, количествено определяне и управление на рисковете, свързани с критични информационни инфраструктури на национално равнище?	1	Използвате ли схема за сертифициране на сигурността или процедура за квалифициране за оценка на доставчиците на услуги, които работят с ООУ? Напр. доставчици на услуги в областта на разкриване на инциденти, реагиране на инциденти, одит на киберсигурността, облачни услуги, смарт карти...	1	-	
	8	-		-		Участвате ли в процес на консултации за идентифициране на трансграничните зависимости?	1	Разполагате ли с механизми за измерване на нивото на съответствие на ООУ и доставчиците на цифрови услуги по отношение на базовите мерки за киберсигурност?	0	-	
Цел на НСКС	**#**	**Ниво 1**	**С**	**Ниво 2**	**С**	**Ниво 3**	**С**	**Ниво 4**	**С**	**Ниво 5**	**С**
11 – Защита на критичната информационна инфраструктура, ООУ и доставчик на цифрови услуги	9					Разполагате ли с едно звено за контакт, отговорно за координирането на въпроси, свързани със сигурността на мрежовите и информационните системи на национално ниво и за трансграничното сътрудничество на нивото на Съюза?	1	Имате ли някакви разпореждания, които да гарантират непрекъснатостта на услугите, предоставяни от критични информационни инфраструктури? Напр. очакване на криза, процедури за възстановяване на критични информационни системи, непрекъснатост на работата без ИТ, процедури за архивиране на въздушни пропуски...	0		
	10					Определяте ли базови мерки за киберсигурност (задължителни или насоки) за доставчиците на цифрови услуги и всички сектори, посочени в приложение II към Директива (ЕС) 2016/1148 за мрежова и информационна сигурност?	1				
	11	-		-		Предоставяте ли инструменти или методологии за откриване на кибер инциденти?	1	-		-	

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
12 – Отговор на киберпрестъпността	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Извършвали ли сте проучване за идентифициране на изискванията за прилагане на закона (правно основание, ресурси, умения...) за ефективно справяне с киберпрестъпността?	1	Вашата национална правна рамка напълно ли е съобразена със съответната правна рамка на ЕС, включително Директива 2013/40/ЕС относно атаките срещу информационните системи? Напр. незаконен достъп до информационни системи, незаконна намеса в системата, незаконна намеса в данните, незаконно прекъсване, инструменти, използвани за извършване на престъпления...	1	Имате ли екипи, посветени на справянето с киберпрестъпления в прокуратурата?	1	Събирате ли статистически данни съгласно разпоредбите на член 14, параграф 1 от Директива 2013/40/ЕС (Директива относно атаките срещу информационните системи)?	1	Имате ли междуинституционални обучения или семинари за обучение за ПО, съдии, прокурори и национални/правителствени ЕРИКС на национално и/или на многостранно ниво?	1
	2	Извършвали ли сте проучване за идентифициране на изискванията за прокурори и съдии (правно основание, ресурси, умения...) за ефективно справяне с киберпрестъпността?	1	Имате ли каквато и да е правна разпоредба, която разглежда кражбата на самоличност и кражбата на лични данни онлайн?	1	Имате ли определен бюджет, разпределен за звена, които се занимават с киберпрестъпления?	1	Събирате ли отделни статистически данни за киберпрестъпността? Напр. оперативна статистика, статистика за тенденциите в киберпрестъпността, статистиката за приходите от киберпрестъпления и причинени щети...	1	Участвате ли в координирани действия на международно ниво за спиране на престъпните дейности? Напр. проникване на престъпни хакерски форуми, организирани киберпрестъпни групи, тъмни уеб пазари и сваляне на ботмрежи...	1
	3	Подписала ли е Вашата държава Конвенцията от Будапеща на Съвета на Европа за престъпления в кибернетичното пространство?	1	Имате ли каквато и да е правна разпоредба, която регламентира онлайн интелектуалната собственост и нарушенията на авторското право?	1	Създадохте ли централен орган/субект, който да координира дейностите в областта на борбата с киберпрестъпността?	1	Оценявате ли адекватността на обучението, предоставено на ПО, съдебната система и персонала на ЕРИКС на държавите за справяне с киберпрестъпността?	1	Има ли ясно разделение на задълженията в ЕРИКС, ПО и съдебната система (прокурори и съдии), когато те си сътрудничат за реагиране на киберпрестъпления?	1

	4			Имате ли някакви правни разпоредби относно онлайн тормоза или кибертормоза?	1	Установихте ли механизми за сътрудничество между съответните национални институции, участващи в борбата с киберпрестъпленията, включително правоприлагащите национални ЕРИКС?	1	Извършвате ли редовни оценки, за да гарантирате, че разполагате с достатъчно ресурси (човешки, бюджет и инструменти), посветени на звената за киберпрестъпност в рамките на ПО?	1	Улеснява ли вашата регулаторна рамка сътрудничеството между ЕРИКС/ПО и съдебната система (прокурори и съдии)?	1
Цел на НСКС	**#**	**Ниво 1**	**C**	**Ниво 2**	**C**	**Ниво 3**	**C**	**Ниво 4**	**C**	**Ниво 5**	**R**
12 — Отговор на киберпрестъпността	5			Имате ли някакви правни разпоредби относно свързаните с компютърни измами? Напр. спазване на разпоредбите на Конвенцията от Будапеща на Съвета на Европа за престъпления в кибернетичното пространство	1	Сътрудничите ли и споделяте информация с други държави членки в областта на борбата с киберпрестъпността?	1	Извършвате ли редовни оценки за гарантиране, че разполагате с достатъчно ресурси (човешки, бюджет и инструменти), определени за отделите за киберпрестъпност в рамките на прокуратурата?	1	Участвате ли в изграждането и поддържането на стандартизирани инструменти и методологии, формуляри и процедури, които трябва да бъдат споделяни със заинтересованите страни от ЕС (ПО, ЕРИКС, ENISA, Европейски център за борба с киберпрестъпността на Европол...)?	1
	6	-		Имате ли правна разпоредба относно закрилата на детето онлайн? Напр. спазване на разпоредбите на Директива 2011/93/ЕС и Конвенцията от Будапеща на Съвета на Европа за престъпления в кибернетичното пространство...	1	Сътрудничите ли и споделяте ли информация с агенциите на ЕС (например, Европейски център за борба с киберпрестъпността на Европол, Евроюст, ENISA) в областта на борбата срещу киберпрестъпността?	1	Имате ли звена специализирани съдилища или специализирани съдии, които да се занимават с киберпрестъпления?	1	Имате ли някакви усъвършенствани механизми, които да възпират хората от това да бъдат привлечени или замесени в киберпрестъпност?	0
	7	-		Установихте ли оперативно национално звено за контакт с цел обмен на информация и отговор на спешни искания за информация от други държави членки във връзка с престъпленията, посочени в Директива 2013/40/ЕС (Директива относно атаките срещу информационните системи)?	1	Имате ли адекватни инструменти за справяне с киберпрестъпността? Напр. таксономията на киберпрестъпността и класификацията, инструменти за събиране на електронни доказателства, инструменти за компютърни криминалисти, надеждни платформи за споделяне...	1	Имате ли някакви разпореждания, посветени на предоставянето на подкрепа и помощ на жертвите на киберпрестъпления (общи потребители, МСП, големи дружества)?	1	Използва ли Вашата държава плана на ЕС и/или Протокола за реагиране при извънредни ситуации, свързани с правоприлагане на ЕС (ПР ИСП ЕС), за да реагира ефективно при широкомащабни кибер инциденти?	0

	8			Вашият правоприлагащ орган включва ли специално звено за киберпрестъпления?	1	Имате ли стандартни оперативни процедури за работа с електронни доказателства?	1	Създали ли сте междуинституционална рамка и механизми за сътрудничество между всички заинтересовани страни (напр. ПО, национален ЕРИКС, съдебни общности), включително частния сектор (напр. оператори на основни услуги, доставчици на услуги) за отговор на кибератаки?	1	-	
	9			Определихте ли, в съответствие с член 35. Конвенция от Будапеща, звено за контакт 24/7?	1	Участва ли Вашата държава във възможностите за обучение, предлагани и/или подкрепени от агенциите на ЕС (напр. Европол, Евроюст, OLAF, CEPOL, ENISA)?	0	Вашата регулаторна рамка улеснява ли сътрудничеството между ЕРИКС и ПО?	1	-	
Цел на НСКС	**#**	**Ниво 1**	**С**	**Ниво 2**	**С**	**Ниво 3**	**С**	**Ниво 4**	**С**	**Ниво 5**	**С**
12 – Отговор на киберпрестъпността	10	-		Определихте ли оперативно национално звено за контакт 24/7 за Протокола за реагиране при извънредни ситуации, свързани с правоприлагане на ЕС (ПР ИСП ЕС) за отговор на големи кибератаки?	1	Възнамерява ли вашата държава да приеме втория допълнителен протокол към Конвенцията от Будапеща на Съвета на Европа за престъпления в кибернетичното пространство?	0	Разполагате ли с механизми (например инструменти, процедури) за улесняване на обмена на информация и сътрудничеството между ЕРИКС/ПО и евентуално съдебната система (прокурори и съдии) в областта на борбата срещу киберпрестъпленията?	1	-	
	11			Осигурявате ли редовно специализирано обучение на заинтересованите страни, участващи в борбата с киберпрестъпността (ПО, съдебната система, ЕРИКС)? Напр. обучителни сесии относно подаването/преследването на киберпрестъпността, обучения за събиране на електронни доказателства и осигуряване на почтеност по цялата дигитална верига на арест и компютърни криминалисти, наред с другото	1						
	12			Ратифицирала ли е/присъединила ли се е Вашата държава към Конвенцията от Будапеща на Съвета на Европа за престъпления в кибернетичното пространство?	1			-	-	-	

	13	-	Подписала ли е и ратифицирала ли е Вашата държава Допълнителния протокол (криминализиране на актове от расистки и ксенофобски характер, извършени чрез компютърни системи) към Конвенцията от Будапеща на Съвета на Европа за престъпления в кибернетичното пространство?	0	-	-	-	-	-	

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
13 – Създаване на механизми за докладване на инциденти	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Разполагате ли с неформални механизми за обмен на информация относно инциденти с киберсигурност между частни организации и национални органи?	1	Имате ли схема за докладване на инциденти за всички сектори съгласно приложение II към Директивата за мрежова и информационна сигурност?	1	Имате ли задължителна схема за докладване на инциденти, която функционира на практика?	1	Имате ли хармонизирана процедура за секторни схеми за докладване на инциденти?	1	Създавате ли годишен доклад за инцидентите?	1
	2	-		Приложихте ли изискванията за уведомяване за доставчиците на телекомуникационни услуги в съответствие с член 40 от Директивата (ЕС 2018/1972)? Директивата изисква държавите членки да гарантират, че доставчиците на обществени електронни съобщителни мрежи или на публично достъпни електронни съобщителни услуги уведомяват незабавно компетентния орган за свързан със сигурността инцидент, който е оказал значително въздействие върху функционирането на мрежи или услуги.	1	Съществува ли механизъм за координация/сътрудничество за задължения за докладване на инциденти по отношение на Общия регламент относно защитата на данните, Директивата за мрежова и информационна сигурност, член 40 (предишен член 13а) и електронната идентификация и удостоверителните услуги?	1	Имате ли схема за докладване на инциденти за сектори, различни от тези по Директивата за мрежова и информационна сигурност?	1	Съществуват ли каквито и да е доклади за положението във връзка с киберсигурността или други видове анализи, изготвени от лицето, което получава докладите за инциденти?	1

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
13 – Създаване на механизми за докладване на инциденти	3	-		Изпълнихте ли изискванията за уведомяване за доставчиците на доверителни услуги в съответствие с член 19 от Регламента относно електронната идентификация (Регламент (ЕС) № 910/2014)? Член 19 изисква, наред с другите изисквания, доставчиците на доверителни услуги да уведомяват надзорния орган за значителни инциденти/нарушения.	1	Разполагате ли с подходящи инструменти за гарантиране на поверителността и целостта на информацията, споделена чрез различните канали за докладване?	1	Измервате ли ефективността на процедурите за докладване на инциденти? *Напр.* показатели за инциденти, които са били докладвани по съответните канали, времето на доклада за инцидент...	1	-	
	4	-		Приложихте ли изискванията за уведомяване за доставчиците на цифрови услуги в съответствие с член 16 от Директивата за мрежова и информационна сигурност? Член 16 изисква доставчиците на цифрови услуги да уведомяват компетентния орган или националния ЕРИКС без неоправдано забавяне за всеки инцидент със значително въздействие върху предоставянето на услуга, както е посочено в приложение III, която предлагат в рамките на Съюза.	1	Имате ли платформа/инструмент за улесняване на процеса на докладване?	0	Имате ли обща таксономия на национално ниво за класификация на инцидентите и категориите първопричини?	0	-	

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
14 – Укрепване на неприкосновеността на личния живот и защитата на данните	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Провеждали ли сте проучвания или анализи, за да определите области на подобрение, за да защитите по-добре правата на неприкосновеността на личния живот на гражданите?	1	Участва ли националният орган за защита на данните в области, свързани с киберсигурността (например разработване на нови закони и подзаконови актове за киберсигурност, определени минимални мерки за сигурност)?	1	Насърчавате ли най-добрите практики по отношение на мерките за сигурност и защитата на данните чрез план за публичния и/или частния сектор?	1	Извършвате ли редовни оценки за гарантиране, че разполагате с достатъчно ресурси (човешки, бюджет и инструменти), определени за органа за защита на данните?	1	Разполагате ли с механизми за наблюдение на последните технологични развития за адаптиране на съответните насоки и правни разпоредби/задължения?	1
	2	Разработихте ли правно основание на национално ниво за прилагане на Общия регламент относно защитата на данните (Регламент ЕС № 2016/679)? Напр. запазване или въвеждане на по-специфични разпоредби или ограничения на правилата на регламента	0	-		Стартирате ли програми за повишаване на осведомеността и за обучение по тази тема?	1	Насърчавате ли организациите и предприятията да бъдат сертифицирани по ISO/IEC 27701:2019 относно Системата за управление на личните данни (СУЛД)?	1	Участвате ли активно/насърчавате ли инициативи за научно-изследователска и развойна дейност по отношение на технологиите за подобряване на защитата на личния живот (PET)?	0
	3	-		-		Координирате ли процедурите за докладване на инциденти с органа за защита на данните?	1	-		-	
	4	-		-		Насърчавате ли и подкрепяте ли разработването на технически стандарти за сигурността на информацията и неприкосновеността на личния живот? Пригодени ли са специално към малките и средните предприятия (МСП)?	0	-		-	

	5	-		-		Предоставяте ли практически и мащабируеми насоки в подкрепа на различни видове администратори на лични данни за изпълнение на законовите изисквания и задължения за защита на неприкосновеността на личния живот и данните?	0	-		-

4.1.4 Клъстер #4: Сътрудничество

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
15 – Създаване на публично-частно партньорство (ПЧП)	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Съществува ли общо разбиране, че ПЧП допринасят за повишаването на нивото на киберсигурност в държавата по различен начин? *Напр.* споделяне на интереси за растежа на индустрията на киберсигурността, сътрудничеството в изграждането на подходяща регулаторна рамка за киберсигурност, насърчаване на научно-изследователска и развойна дейност...	1	Имате ли национален план за действие за създаване на ПЧП?	1	Установихте ли национални публично-частни партньорства?	1	Създадохте ли междусекторни ПЧП?	1	В зависимост от последните технологични и регулаторни развития, можете ли да адаптирате или създадете ПЧП?	1
	2	-		Създавате ли правно или договорно основание (специфични закони, споразумения за поверителност, интелектуална собственост) за обхващане на ПЧП?	1	Създадохте ли специфични за сектора ПЧП?	1	В създадените ПЧП също ли се фокусирате върху публично-публично и частно-частно сътрудничество?	1		
	3	-		-		Осигурявате ли финансиране за създаването на ПЧП?	1	Насърчавате ли ПЧП сред малките и средните предприятия (МСП)?	1	-	

	4	-		-		Публичните институции ръководят ли ПЧП като цяло? *Т.е.* единно звено за контакт от публичния сектор, което управлява и координира ПЧП, публичните органи предварително се споразумяват за това какво искат да постигнат, ясни насоки от публичните администрации относно техните нужди и ограничения за частния сектор...	1	Измервате ли резултатите от ПЧП?	1	-	
	5	-		-		Член ли сте на договорното публично-частно партньорство (ДПЧП) на Европейската организация за киберсигурност (ECSO)?	0	-		-	
Цел на НСКС	**#**	**Ниво 1**	**С**	**Ниво 2**	**С**	**Ниво 3**	**С**	**Ниво 4**	**С**	**Ниво 5**	**С**
15 – Създаване на публично-частно партньорство (ПЧП)	6	-		-		Имате ли едно или няколко ПЧП, които работят по свързани с ЕРИКС дейности?	0	-		-	
	7					Имате ли едно или няколко ПЧП, които работят по въпросите на защитата на критичната информационна инфраструктура?	0				
	8	-		-		Имате ли едно или няколко ПЧП, които работят за повишаване на осведомеността за киберсигурност и развитието на уменията?	0	-		-	

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
16 – Институционализиране на сътрудничеството между публичните агенции	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Имате ли неформални канали за сътрудничество между публични агенции?	1	Имате ли национална схема за сътрудничество, насочена към киберсигурността? *Напр.* консултативни съвети, ръководни групи, форуми, съвети, кибер центрове или експертни групи за срещи	1	Участват ли публичните органи в схемата за сътрудничество?	1	Гарантирате ли, че каналите за сътрудничество, посветени на киберсигурността, съществуват поне между следните публични органи: разузнавателни служби, вътрешни правоприлагащи органи, прокуратура, участници от правителството, националния ЕРИКС и военните?	1	Дали публичните агенции разполагат с единна минимална информация относно последните развития на положението със заплахите и информираността за ситуацията с киберсигурността?	1
	2	-		-		Създадохте ли платформи за сътрудничество за обмен на информация?	1	Измервате ли успехите и ограниченията на различната схема за сътрудничество за насърчаване на ефективното сътрудничество?	1	-	

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
16 – Институционализиране на сътрудничеството между публичните агенции	3	-		-		Определихте ли обхвата на платформите за сътрудничество (например задачи и отговорности, брой области, свързани с въпроса)?	1	-		-	
	4	-		-		Организирате ли годишни срещи?	1	-		-	

	5	-		-		Имате ли механизми за сътрудничество между компетентните органи в географските региони? *Напр.* мрежа от свързани със сигурността кореспонденти по регион, служител по киберсигурност в регионалните икономически камари...	1	-		-	

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
17 – Участие в международно сътрудничество (не само с държавите—членки на ЕС)	а)	Покривате ли целта в настоящата си НСКС или планирате да я покриете в следващото издание?	1	Съществуват ли неформални практики или дейности, които участват в постигането на целта по некоординиран начин?	1	Имате ли план за действие, който е официално определен и документиран?	1	Преглеждате ли плана си за действие по отношение на целта за изпитване на неговото изпълнение?	1	Разполагате ли с механизми, които да гарантират, че планът за действие е динамично адаптиран към развитието на околната среда?	1
	б)			Определихте ли предвидени резултати, водещи принципи или ключови дейности на вашия план за действие?	1	Имате ли план за действие с ясно разпределение на ресурсите и управление?	1	Преглеждате ли плана си за действие по отношение на целта, за да се гарантира, че той е правилно подреден по приоритети и оптимизиран?	1		
	в)			Ако е уместно, прилага ли се вашият план за действие и вече е в сила в ограничен обхват?	0						
	1	Имате ли международна стратегия за ангажимент?	1	Имате ли споразумения за сътрудничество с други държави (двустранни, многостранни) или партньори в други държави? *Напр.* споделяне на информация, изграждане на капацитет, подпомагане...	1	Обменяте ли информация на стратегическо ниво? *Напр.* политика на високо ниво, възприемане на риска...	1	Участват ли националните публични агенции за киберсигурност във Вашата държава в схеми за международно сътрудничество?	1	Водите ли дискусии по една или много теми в рамките на многостранни споразумения?	1
	2	Имате ли неформални канали за сътрудничество с други държави?	1	Имате ли едно звено за контакт, което може да упражнява функция за връзка за гарантиране на трансгранично сътрудничество с органите на държавите членки (група за сътрудничество, мрежа на ЕРИКС...)?	1	Обменяте ли информация на тактическо ниво? *Напр.* бюлетин на участниците, свързани със заплахата, центрове за споделяне и анализ на информация, тактика, техника и процедури...	1	Оценявате ли редовно резултатите от инициативите за международно сътрудничество?	1	Водите ли дискусии по една или много теми в рамките на международни договори или конвенции?	1

Цел на НСКС	#	Ниво 1	С	Ниво 2	С	Ниво 3	С	Ниво 4	С	Ниво 5	С
17 – Участие в международно сътрудничество (не само с държавите—членки на ЕС)	3	Изразявало ли е обществено ръководство намерение да участва в международно сътрудничество в областта на киберсигурността?	1	Имате ли определени хора, които участват в международно сътрудничество?	1	Обменяте ли информация на оперативно ниво? *Напр.* информация за оперативна координация, текущи инциденти, първоначална оперативна готовност...	1	-		Водите ли дискусии или преговори по една или много теми в рамките на международни експертни групи? *Напр.* Глобалната комисия за стабилност на киберпространството (GCSC), група за сътрудничество за мрежова и информационна сигурност на ENISA, Група на правителствени експерти на ООН по информационна сигурност (GGE)...	1
	4	-		-		Участвате ли в международни дейности по киберсигурност?	1	-		-	
	5	-		-		Участвате ли в международни инициативи за изграждане на капацитет? *Напр.* обучения, развитие на умения, изготвяне на стандартни процедури...	0	-		-	
	6	-		-		Подписали ли сте споразумения за взаимопомощ с други държави? *Напр.* дейности на ПО, съдебни производства, взаимопомощ на възможностите за реагиране на инциденти, споделяне на свързани с киберсигурността активи...	0	-		-	
	7	-		-		Подписали или ратифицирали ли сте международни договори или конвенции в областта на киберсигурността? *Напр.* Международен етичен кодекс за информационна сигурност, Конвенция за киберпрестъпления	0	-		-	

4.2 НАСОКИ ЗА ИЗПОЛЗВАНЕ НА РАМКАТА

Настоящият раздел има за цел да предостави на държавите членки някои насоки и препоръки за изготвяне на рамката и за попълване на въпросника. Изброените по-долу препоръки произтичат главно от обратната връзка, събрана от интервютата с представителите на държавите членки:

- **Предвиждане на координационни дейности за събиране на данни и консолидиране на данни.** Повечето държави членки признават, че извършването на такова самооценка следва да отнеме около 15 дни за всеки отделен служител. За да се извърши самооценка, ще трябва да бъдат потърсени широк кръг от различни заинтересовани страни. Поради това се препоръчва да се отдели време за фазата на подготовка за идентифициране на всички заинтересовани страни в държавните органи, публичните агенции и частния сектор.
- **Идентифициране на централен орган, който отговаря за завършването на самооценката на национално ниво.** Тъй като събирането на материали за всички показатели на НРОВ може да включва много заинтересовани страни, се препоръчва централен орган или агенция да има за задача да извърши самооценката чрез свързване и координиране с всички заинтересовани страни.
- **Използвайте дейността по оценяване като начин за споделяне и комуникация по теми, свързани с киберсигурността.** Извлечените от държавите членки поуки показаха, че обсъжданията (независимо под формата на индивидуални интервюта или колективни семинари) са добра възможност за насърчаване на диалога по въпросите на киберсигурността и за споделяне на общи възгледи и области на подобрение. В допълнение към осветяването на ключовите постижения, споделянето на резултати може също да помогне за насърчаване на свързаните с киберсигурността теми.
- **Използвайте НСКС като обхват за избор на целите, предмет на оценката.** 17-те цели, които съставят НРОВ, са изградени въз основа на целите, които обикновено са обхванати от държавите членки в техните НСКС. Целите, обхванати като част от НСКС, следва да се използват като средство за разширяване на обхвата на оценката. НСКС обаче не следва да ограничава оценката. Тъй като НСКС естествено набляга на приоритетите, някои области са умишлено пропуснати от нея. Това обаче не означава, че даден капацитет не е налице. Например, в случаите, когато дадена цел е пропусната от НСКС, но когато държавата има възможности за киберсигурност, свързани с тази цел, може да се извърши оценка на тази цел.
- **Когато обхватът на НСКС се развива, следва да гарантирате, че тълкуването на оценката остава в съответствие с развитието на НСКС.** Жизненият цикъл на НСКС е многогодишен процес. НСКС на някои държави членки обикновено се прилагат с пътна карта от 3 до 5 години с промени в обхвата между две последователни издания на НСКС. В тази връзка трябва да се обърне специално внимание при представянето на резултатите от самооценка между две издания на НСКС: промените на обхвата може в действителност да повлияят на окончателната оценка на зрелостта. Препоръчително е да се сравняват оценките на пълния обхват на стратегическите цели от една година с друга (*m.e.* общия резултат).

Напомняне за механизма за оценяване — пример за коефициент на покритие
Механизмът за оценяване включва две нива на оценки:
(i) изчислено **общо коефициент на покритие** въз основа на пълния списък на стратегическите цели, които присъстват в рамката за самооценка; и
(ii) **общо специфично коефициент на покритие** въз основа на стратегически цели, избрани от държавата членка (обикновено съответстващо на целите, които са налице в НСКС на конкретната държава).

По проект (вж. раздел 3.1 за механизма за оценяване), общото специфично коефициент на покритие ще бъде равно или по-голямо от общото коефициент на покритие, тъй като последното може да включва цели, които не са обхванати от държавата членка, като по този начин се намалява общото коефициент на покритие. Когато държава членка добави нова цел, общото коефициент на покритие ще се увеличи (т.е. повече обхванати показатели за зрялост), докато общата специфична зрялост може да намалее (в случай, че новата добавена цел е в начален етап и следователно има ниско ниво на зрялост).

- **При попълването на въпросника за самооценка, имайте предвид, че основната цел е да се подкрепят държавите членки в изграждането на капацитет за киберсигурност.** Следователно, при попълването на самооценката, дори и да е трудно в някои ситуации да се отговори на въпроса по определен начин, се препоръчва да изберете отговора, който е общоприет в най-голяма степен. Ако, например, отговорът на въпрос е „ДА“ в определен обхват, но „НЕ“ е в друг обхват, държавите членки следва да имат предвид, че отговорът „НЕ“ изисква действие: или план за възстановяване, или план за действие в област на подобрение, който трябва да бъде взет предвид в бъдещото развитие.

5. СЛЕДВАЩИ СТЪПКИ

5.1 БЪДЕЩИ ПОДОБРЕНИЯ

По време на интервюта с представители на държавите членки и по време на етапа на проучване на бюро бяха определени също следните препоръки за подобряване на настоящата национална рамка за оценка на възможностите като потенциално бъдещо развитие:

- **Разработване на системата за оценяване, за да се даде възможност за по-голяма точност.** Например, може да се въведе процент на покритието вместо двоичния отговор „ДА/НЕ“ за по-добро отчитане на сложността на консолидирането на възможностите на национално ниво. Като първа стъпка беше избран прост подход с отговори „ДА/НЕ“.
- **Въвеждане на количествени показатели за измерване на ефективността на НСКС на държавите членки.** Всъщност националната рамка за оценка на възможностите акцентира върху оценката на нивото на зрялост на възможностите за киберсигурност на държавите членки. Това може да бъде допълнено от показатели за измерване на ефективността на дейностите и плановете за действие, изпълнявани от държавите членки за изграждане на тези възможности. Не изглежда реалистично да се създадат подобни показатели за ефективност на настоящия етап, като се има предвид, че е налице: малко обратна връзка от областта, трудното намиране на значими показатели, които свързват резултатите с изпълнението на НСКС, както и трудно изграждане на реалистични показатели, които впоследствие могат да бъдат събрани. Това обаче остава тема за бъдеща работа.
- **Преминаване от самооценка към подход за оценка.** Потенциално бъдещо развитие на рамката може да бъде преминаването към подход за оценка, за да се оцени зрелостта на възможностите за киберсигурност на държавите членки по по-последователен начин. Извършването на оценката от трета страна може наистина да позволи да се сведат до минимум потенциалните предразсъдъци.

ПРИЛОЖЕНИЕ А - ПРЕГЛЕД НА РЕЗУЛТАТИТЕ ОТ ПРОУЧВАНИЯТА НА БЮРО

Приложение А съдържа обобщение на предишна работа на ENISA за НСКС и преглед на съответните публично достъпни модели на зрялост за капацитета за киберсигурност. При подбора и прегледа на моделите се вземат предвид следните допускания:

- Не всички модели се основават на строга научно - изследователска методология;
- Структурата и резултатите от моделите не винаги са подробно обяснени с ясни връзки между различните елементи, които характеризират всеки модел;
- Някои модели не предлагат информация за процеса на развитие, структурата и методологията за оценка;
- Други модели и инструменти, които открихме, не предлагат никаква информация относно структурата и съдържанието и следователно не са изброени; и
- Изборът на моделите за преглед се основава на географско покритие. Основният акцент ще бъде върху моделите на зрялост за капацитета за киберсигурност, изградени за оценка на ефективността на европейските държави. Важно е обаче да се разшири географското покритие, за да се анализират добрите практики при изграждането на модели на зрялост по целия свят.

Този систематичен преглед на съответните публично достъпни модели на зрялост за капацитета за киберсигурност беше извършен чрез персонализирана рамка за анализ въз основа на методиката, определена от Becker за разработването на модели на зрялост[22]. За всеки съществуващ модел за зрялост бяха анализирани следните елементи:

- **Име на модела за зрялост:** Име на модела за зрялост и основни източници;
- **Източник на институцията:** Институцията, публична или частна, която отговаря за създаването на модела;
- **Обща цел и цел:** цялостния обхват на модела и планираната(ите) цел(и);
- **Брой и определение на нива:** броя на нивата на зрялост на модела, както и общото им описание;
- **Брой и име на атрибутите:** Броят и името на атрибутите, които използва моделът на зрялост. Анализът на атрибутите има цел с три аспекта:
  - разбивка на модела за зрялост на лесно разбираеми раздели;
  - обединяване на няколко атрибути в клъстери от атрибути, които отговарят на една и съща цел; и
  - представяне на различни гледни точки на предмета на нивото на зрялост.
- **Метод на оценка:** Метода на оценка на модела за зрялост;

[22] J. Becker, R. Knackstedt, и J. Pöppelbuß, „Разработване на модели на зрялост за управление на ИТ: Процедурен модел и неговото приложение," Business & Information Systems Engineering, том 1, № 3, стр. 213—222, юни 2009 г.
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- **Представяне на резултатите**: Дефиниране на метода на визуализация за резултатите от модела за зрялост. Логиката зад тази стъпка е, че моделите на зрялост са склонни да се провалят, ако са твърде сложни и следователно начинът на представяне трябва да отговаря на практическите нужди.

Предишна работа по НСКС

ENISA публикува два документа по темата за НСКС през 2012 г. като част от ранните си усилия. На първо място, „Практически наръчник за фазата на развитие и изпълнение на НСКС“[23] предложи набор от конкретни действия за ефективното прилагане на НСКС и представя жизнения цикъл на НСКС в четири фази: развитие на стратегия, изпълнение на стратегия, оценка на стратегия и поддръжка на стратегия. На второ място, документ, наречен „Определяне на курса за национални усилия за укрепване на сигурността в киберпространството“[24] очерта състоянието на стратегиите за киберсигурност в рамките на ЕС и извън него през 2012 г. и предложи държавите членки да определят общи теми и различия между своите НСКС.

Първата рамка на ENISA за оценка на НСКС на държава членка е публикувана през 2014 г[25]. Тази рамка съдържа препоръки и добри практики, както и набор от инструменти за изграждане на капацитет за оценка на НСКС (*напр.* определени цели, ресурси, резултати, ключови показатели за ефективност...). Тези инструменти са адаптирани към различните нужди на държавите на различни нива на зрялост при стратегическото им планиране. Същата година ENISA публикува „Онлайн интерактивна карта за НСКС“[26], която позволява на потребителите бързо да се консултират с НСКС на всички държави членки и държавите от ЕАСТ, включително с техните стратегически цели и добри примери за изпълнение. Разработена за първи път като база от данни на НСКС (2014 г.), тя е актуализирана с примери за изпълнение през 2018 г. и от 2019 г. насам, картата сега действа като информационен център за централизиране на данни, предоставени от държавите членки за техните усилия за повишаване на националната киберсигурност.

Публикуван през 2016 г., „Наръчник за добри практики на НСКС“[27] идентифицира петнадесет стратегически цели. Настоящото ръководство анализира също така статута на изпълнение на НСКС на всяка държава членка и посочва различни пропуски и предизвикателства по отношение на това изпълнение.

През 2018 г. ENISA публикува „Национален инструмент за оценка на стратегиите за киберсигурност“[28]: интерактивен инструмент за самооценка, който да помогне на държавите членки да оценят стратегическите си приоритети и цели, свързани с техните НСКС. Чрез набор от прости въпроси този инструмент предоставя на държавите членки конкретни препоръки за изпълнението на всяка цел. И накрая, „Добри практики в иновациите в областта на киберсигурността в рамките на НСКС“[29], публикувани през

[23] НСКС: Практическо ръководство за развитие и изпълнение (ENISA, 2012 г.)
https://www.enisa.europa.eu/publications/national-cyber-security-strategies-an-implementation-guide
[24] НСКС: Определяне на курса за национални усилия за укрепване на сигурността в киберпространството (ENISA, 2012 г.)
https://www.enisa.europa.eu/publications/cyber-security-strategies-paper
[25] Рамка за оценка за НСКС (ENISA, 2014 г.)
https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies
[26] Национални стратегии за киберсигурност — Интерактивна карта (ENISA, 2014 г., актуализирана през 2019 г.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
[27] Настоящият документ актуализира ръководството от 2012 г. Наръчник за добри практики на НСКС: Създаване и прилагане на национални стратегии за киберсигурност (ENISA, 2016 г.)
https://www.enisa.europa.eu/publications/ncss-good-practice-guide
[28] Национален инструмент за оценка на стратегиите за киберсигурност (2018 г.)
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool
[29] https://www.enisa.europa.eu/publications/good-practices-in-innovation-on-cybersecurity-under-the-ncss-1

2019 г., представят темата за иновациите в киберсигурността в рамките на НСКС. Документът излага предизвикателства и добри практики в различните иновационни измерения, както е възприето от експертите по предмета, в помощ на разработването на бъдещи иновативни стратегически цели.

A.1 Модел за зрялост на капацитета за киберсигурност за държавите (МЗК)

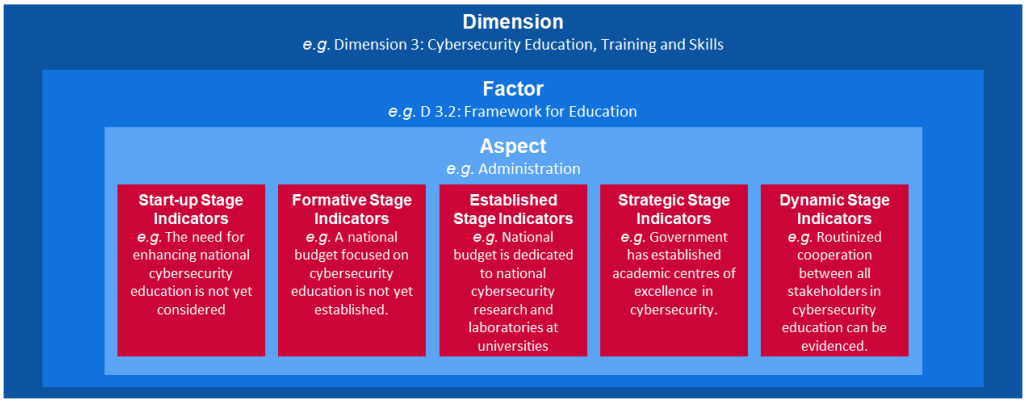
Моделът на зрялост на капацитета за киберсигурност за държавите (МЗК) е разработен от Глобалния център за капацитет за киберсигурност (Център за капацитет), част от Oxford Martin School към Оксфордския университет. Целта на Центъра за капацитет е да увеличи мащаба и ефективността на изграждането на капацитет за киберсигурност както в Обединеното кралство, така и в международен план чрез внедряването на Модела на зрялост на капацитета за киберсигурност (МЗК). МЗК е пряко насочен към държави, които желаят да увеличат своя национален капацитет за киберсигурност. Първоначално внедрен през 2014 г., МЗК беше преразгледан през 2016 г. след използването му при прегледа на 11 национални капацитета за киберсигурност.

Атрибути/Измерения

МЗК счита, че капацитетът за киберсигурност включва **пет измерения** , които представляват клъстерите на капацитета за киберсигурност. Всеки клъстер представлява различна изследователска „лупа“, чрез която може да бъде проучен и разбран капацитетът за киберсигурност. В рамките на петте измерения **факторите** описват детайлите за притежаване на капацитет за киберсигурност. Тези детайли са елементи, които допринасят за повишаване на зрелостта на капацитета за киберсигурност във всяко измерение. За всеки фактор няколко **аспекта** представляват различни компоненти на фактора. Аспектите представляват организационен метод за разделяне на показатели на по-малки клъстери, които са по-лесни за разбиране. След това всеки аспект се оценява чрез **показатели** за описание на стъпките, действията или градивните елементи, които са показателни за конкретен етап на зрялост (определен в следващия раздел) в рамките на отделен аспект, фактор и измерение.

Посочените по-горе термини могат да бъдат разположени, както е показано на фигурата по-долу.

Фигура 4: Пример на показатели заМЗК



Dimension e.g. Dimension 3: Cybersecurity Education, Training and Skills	Измерение напр. Измерение 3: Образование за киберсигурност, обучение и умения
Factor e.g. D 3.2: Framework for Education	Фактор напр. Г 3.2: Рамка за образование
Aspect e.g. Administration	Аспект напр. администриране

Start-up Stage Indicators e.g. The for enhancing national cybersecurity education is not yet considered	Показатели за начален етап напр. въпросът за подобряване на образованието по национална киберсигурност все още не е разгледан
Formative Stage Indictors e.g. A national budget focused on cybersecurity education is not yet established	Показатели за формиращ етап напр. национален бюджет за образование по киберсигурност все още не е заделен
Established Stage Indicators e.g. National budget is dedicated to national cybersecurity research and laboratories at universities	Показатели за етап на създаване напр. националният бюджет е разпределен за национални проучвания и лаборатории за киберсигурност в университети
Strategic Stage Indicators e.g. Government has established academic center of excellence in cybersecurity education can be evidenced.	Показатели за стратегически етап напр. може да бъде удостоверено, че правителството е създало отличен академичен център по киберсигурност.
Dynamic Stage Indicators e.g. Routinized cooperation between all stakeholder	Показатели за динамичен етап напр. рутинно сътрудничество между всички заинтересовани лица

Петте измерения са описани по-долу:

i Разработване на политика и стратегия за киберсигурност (6 фактора);
ii Насърчаване на отговорната култура на киберсигурност в обществото (5 фактора);
iii Създаване на знания за киберсигурност (3 фактора);
iv Създаване на ефективни правни и регулаторни рамки (3 фактора); и
v Контролиране на рисковете чрез стандарти, организации и технологии (7 фактора).

Нива на зрялост

МЗК използва **5 нива на зрялост** за определяне до каква степен дадена държава е напреднала по отношение на определен фактор/аспект на капацитета за киберсигурност. Тези нива служат като моментна снимка на съществуващите възможности за киберсигурност:

- **Започване**: На този етап или не съществува зрялост на киберсигурността, или тя е на много начален етап по естество. Може да има първоначални обсъждания относно изграждането на капацитет за киберсигурност, но не са предприети конкретни действия. На този етап липсват видими доказателства;
- **Формиране**: Някои характеристики на аспектите са започнали да растат и да бъдат формулирани, но могат да бъдат ad hoc, дезорганизирани, зле дефинирани или просто „нови“. Доказателствата за тази дейност обаче могат да бъдат ясно показани;
- **Създаване**: Елементите на аспекта са налице и работят. Няма обаче добре обмислено разглеждане на относителното разпределение на ресурсите. По отношение на „относителните“ инвестиции в различните елементи на аспекта не се взема компромисно решение. Въпреки това, аспектът е функционален и определен.
- **Стратегически етап**: Направени са избори за това кои части от аспекта са важни и които са по-малко важни за конкретната организация или нация. Стратегическият етап отразява факта, че този избор е направен, в зависимост от конкретните обстоятелства на държавата или организацията; и
- **Динамичен етап**: На този етап съществуват ясни механизми за промяна на стратегията в зависимост от преобладаващите обстоятелства, като например технологията на средата на заплахата, глобалния конфликт или значителна промяна в една област на безпокойство (*напр.* киберпрестъпност или неприкосновеност на личния живот). Динамичните организации са разработили методи за промяна на стратегиите в ход. Бързото вземане на решения, преразпределянето на ресурсите и постоянното внимание към променящата се среда са характерни за този етап.

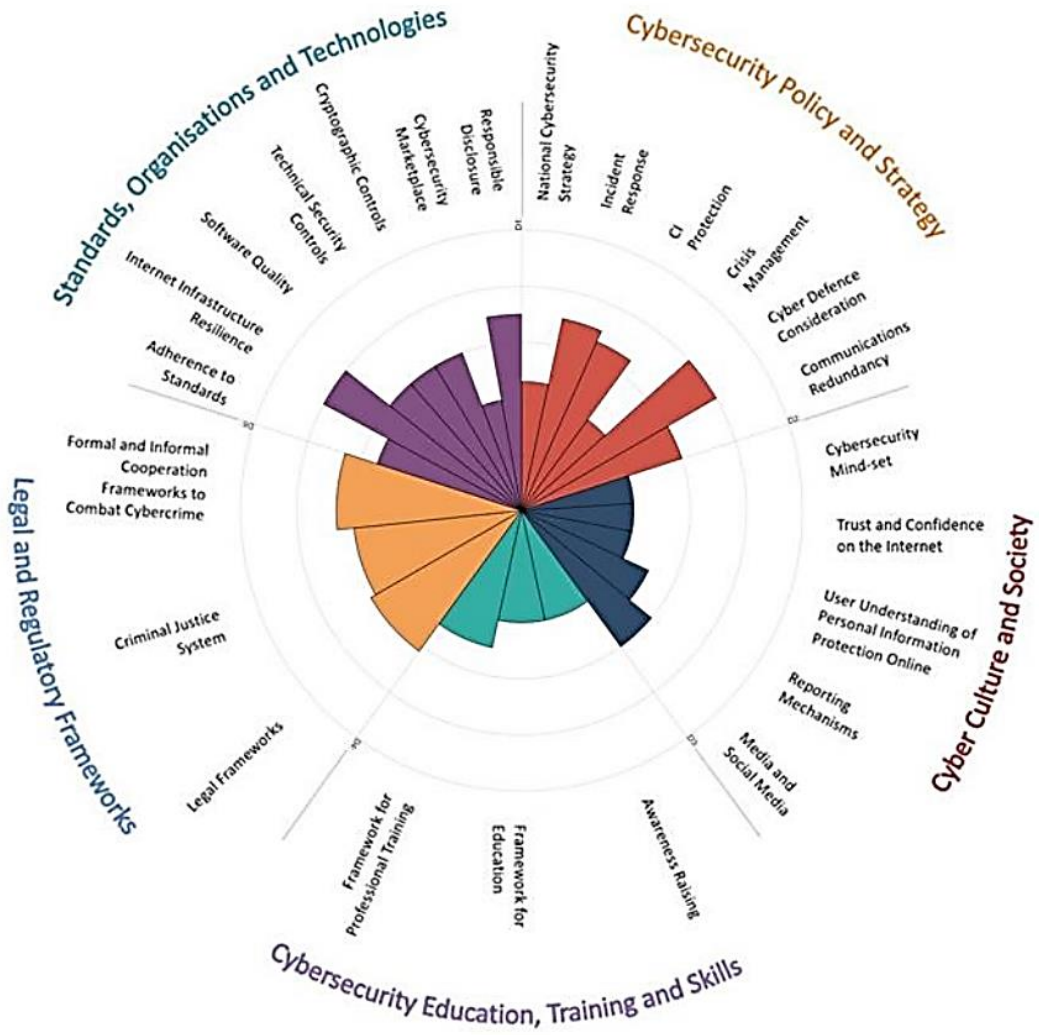
Метод на оценка

Тъй като Центърът за капацитет няма подробно и задълбочено разбиране на всеки местен контекст, в който е внедрен моделът, той работи заедно с международни организации, приемащи министерства или организации в рамките на съответната държава за преглед на зрелостта на капацитета за киберсигурност. За да оцени степента на зрялост на петте измерения, включени в МЗК, Центърът за капацитет и приемащата организация се срещат със съответните заинтересовани страни на държавите от публичния и частния сектор в рамките на 2 или 3 дни за провеждане на фокус групи относно измеренията на МЗК. Всяко измерение се обсъжда най-малко два пъти от различни групи заинтересовани страни. Това представлява предварителния набор от данни за последващата оценка.

Режим или представяне на резултатите

МЗК предоставя преглед на нивото на зрялост на всяка държава чрез радар, състоящ се от пет секции, по една за всяко измерение. Всяко измерение представлява една пета от графиката, с пет етапа на зрялост за всеки фактор, който се простира навън от центъра на графиката; както е показано по-долу, „започването“ е най-близо до центъра на графиката, а „динамичен“ е в периметъра.

Фигура 5 МЗК: Преглед на резултатите



Standards, Organisations and Technologies	Стандарти, организации и технологии

Legal Regulatory Frameworks	Правни регулаторни рамки
Cybersecurity Education, Training and Skills	Образование за киберсигурност, обучение и умения
Cybersecurity Policy and Strategy	Политика и стратегия за киберсигурност
Cyber Culture and Society	Кибер култура и общество
Responsible Disclosure	Отговорно оповестяване
Cybersecurity market place	Място на пазара на киберсигурност
Cryptographic Controls	Криптографски контрол
Technical Security Controls	Контролни механизми за техническа сигурност
Software Quality	Качество на софтуера
Internet Infrastructure Resilience	Устойчивост на интернет инфраструктурата
Adherence to Standards	Спазване на стандарти
Formal and Informal Cooperation Frameworks to Combat Cybercrime	Формални и неформални рамки за сътрудничество за борба с киберпрестъпността
Criminal Justice System	Система за наказателно правосъдие
Legal Frameworks	Правни рамки
Framework for Professional Training	Рамка за професионално обучение
Framework for Education	Рамка за образование
Awareness Raising	Повишаване на осведомеността
Media and Social Medai	Медии и социални медии
Reporting Mechanisms	Механизми за докладване
User Understanding of Personal Information Protection Online	Разбиране на потребителя на защитата на личната информация онлайн
Trust and Confidence on the Internet	Доверие и увереност в Интернет
Cybersecurity Mind-set	Съзнание за киберсигурност
Communications Redundancy	Съкращаване на комуникациите
Cyber Defence Consideration	Разглеждане на киберзащита
Crisis Management	Управление на кризи
CI Protection	Защита на КИ
Incident Response	Отговор на инцидент
National Cybersecurity Strategy	Национална стратегия за киберсигурност

Оксфордското училище „Мартин“ на Глобалния център за капацитет за киберсигурност, Оксфордски университет, 2017 г.

A.2 Модел за зрялост на капацитета за киберсигурност (C2M2)

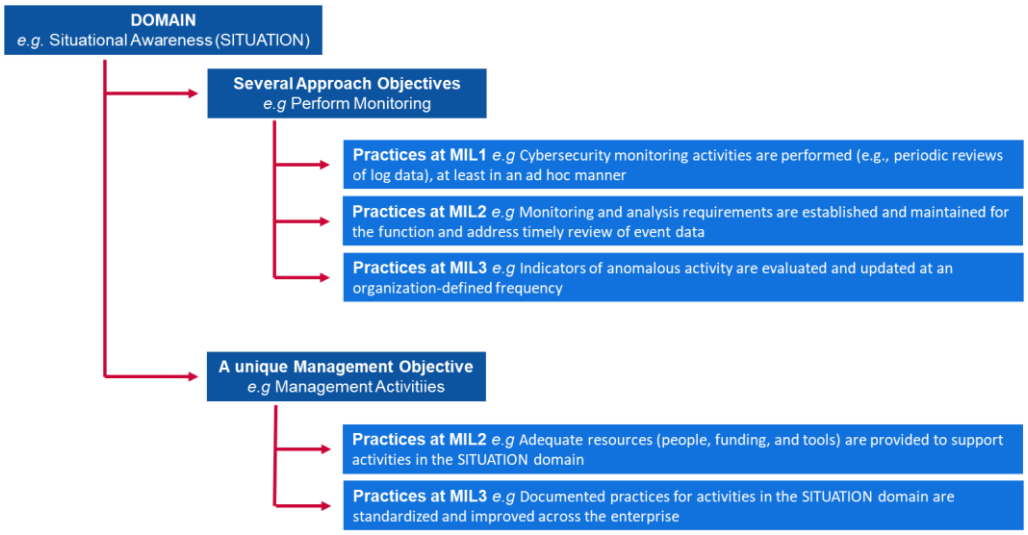
Моделът на зрялост на капацитета за киберсигурност (C2M2) е разработен от Министерството на енергетиката на САЩ в сътрудничество с експерти от частния и публичния сектор. Целта на Центъра за капацитет е да помогне на организации от всички сектори, видове и с различен размер да оценят и направят подобрения в своите програми за киберсигурност и да засилят своята оперативна устойчивост. C2M2 набляга на прилагането и управлението на практиките за киберсигурност, свързани с информацията, активи от информационните технологии (ИТ) и оперативните технологии (ОТ) и средата, в която те оперират. C2M2 определя моделите на зрялост като: „набор от характеристики, атрибути, показатели или модели, които представляват възможност и прогресия в определена дисциплина“. Първоначално внедрен през 2014 г., C2M2 е преразгледан през 2019 г.

Атрибути/Измерения

C2M2 разглежда **десет области**, които представляват логическа група от свързани с киберсигурност практики. Всеки набор от практики представлява дейностите, които една организация може да извършва за създаване и развитие до зрялост на капацитет в областта. След това всяка област е свързана с **уникална цел на управление** и **няколко цели на подхода**. В рамките на подхода и целите на управлението са подробно описани **няколко практики** за описание на институционализираните дейности.

Връзката между тези понятия е обобщена по-долу:

Фигура 6: Пример на показател за C2M2



Domain eg Situational Awareness (SITUATION)	**Област** напр. информираност за ситуацията (СИТУАЦИЯ)
Several Approaches Objectives e.g. Perform Monitoring	**Няколко цели на подходите** напр. извършване на мониторинг
Practices at MIL1 e.g Cybersecurity monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	**Практики на НП31** напр. дейностите за наблюдение на киберсигурността се осъществяват (напр. периодични прегледи на регистрационни данни), най-малко по ad hoc начин
Practices at MIL2 e.g Monitoring and analysis requirement are established and maintained for the function and adress timely review of event data	**Практики на НП32** напр. изискването за мониторинг и анализ се въвежда и поддържа за функцията и отговаря на навременния преглед на данните за събитието
Practices at MIL3 e.g Indicators of anomalous activity are evaluated and updated at an organization-defined frequency	**Практики на НП33**напр. показателите за аномална активност се оценяват и актуализират на определена от организацията честота
A unique Management Objectve e.g. Management Activities	Уникална управленска цел, напр. управленски дейности
Practices at MIL2 e.g Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain	**Практики на НП32**напр. адекватни ресурси (хора, финансиране и инструменти) се предоставят за подпомагане на дейности в областта на СИТУАЦИЯТА
Practices at MIL3 e.g Documented practices for activities in the SITUATION domain are standardized and improved across the entreprise	**Практики на НП33** напр. документирани практики за дейности в областта на СИТУАЦИЯТА са стандартизирани и подобрени в рамките на предприятието

Десетте области са подробно описани по-долу:

i Управление на риска (РИСК);
ii Управление на активите, промяната и конфигурирането (АКТИВ);
iii Управление на самоличността и достъпа (ДОСТЪП);
iv Управление на заплахите и уязвимостта (ЗАПЛАХА);
v Информираност за ситуацията (СИТУАЦИЯ);
vi Реагиране на събития и инциденти (РЕАГИРАНЕ);
vii Управление на веригата за доставки и на външните зависимости (ЗАВИСИМОСТИ);
viii Управление на работната сила (РАБОТНА СИЛА);
ix Архитектура на киберсигурността (АРХИТЕКТУРА);
x Управление на програмата за киберсигурност (ПРОГРАМА).

Нива на зрялост

C2M2 използва **4 нива на зрялост** (наречени нива на показатели за зрялост — НПЗ) за определяне на двойна прогресия на зрелостта: прогресия на подхода и прогресия на управлението. НПЗ варират от НП30 до НП33 и са предназначени да бъдат прилагани независимо за всяка област.

- **НП30**: Практики не се извършват.
- **НП31**: Извършват се първоначални практики, но могат да бъдат ad hoc.
- **НП32**: Характеристики на управлението:
  - Практиките са документирани;
  - Предоставят се адекватни ресурси в подкрепа на процеса;
  - Персоналът, който извършва практиките, има адекватни умения и знания; и
  - Възлагат се отговорност и права за извършване на практиките.

  Характеристика на подхода:
  - Практиките са по-пълни или напреднали отколкото на НП31.
- **НП33**: Характеристики на управлението:
  - Дейностите се ръководят от политики (или други организационни директиви);
  - Целите за изпълнение на дейностите по области се определят и наблюдават с цел проследяване на постигнатите резултати; и
  - Документираните практики за дейности на областите са стандартизирани и подобрени в предприятието.

  Характеристика на подхода:
  - Практиките са по-пълни или напреднали отколкото на НП32.

Метод на оценка

C2M2 е предназначен за използване с **методика за самооценка** и инструментариум (наличен със заявка) за дадена организация за измерване и подобряване на нейната програма за киберсигурност. Самооценка с помощта на инструмента може да бъде завършена за един ден, но инструментариумът може да бъде адаптиран за усилия за по-строга оценка. Освен това C2M2 може да се използва за насочване на разработването на нова програма за киберсигурност.

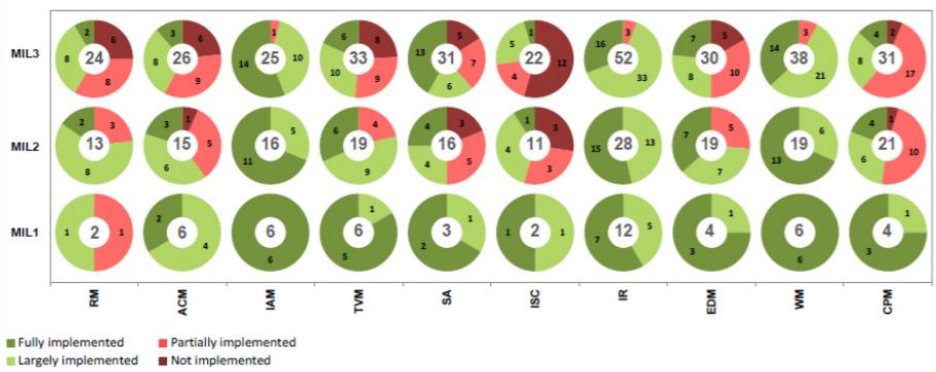
Съдържанието на модела е представено на високо ниво на абстракция, така че да може да бъде интерпретирано от организации от различни видове, структури, размери и индустрии. Широкото използване на модела от даден сектор може да подпомогне сравняването на възможностите за киберсигурност на сектора.

Режим или представяне на резултатите

C2M2 представя доклад за оценка, получен от резултатите от проучването. Докладът представя резултатите от две гледни точки: обективната гледна точка, която показва практически отговори на въпроси от всяка област и неговите цели, и гледната точка на областта, която показва отговори от всички области и НП3. И двете гледни точки се основават на система за представяне, характеризираща се с пай диаграми (или „понички“), по една на отговор и механизъм за оценка на „системата на светофара“. Както е показано в Фигура 7, червените сектори в диаграмата „поничка“ показват броя на въпросите, които са получили анкетни отговори „Не е изпълнено“ (тъмно червено) или „Частично изпълнено“ (светло червено). Зелените сектори показват броя на въпросите, които са получили отговори: „Изпълнено в голяма степен“ (светло зелено) или „Цялостно изпълнено“ (тъмно зелено).

Фигура 7 по-долу е пример за карта за оценка в края на оценката на зрелостта. По оста X са 10-те области на C2M2, а по оста Y — нивата на зрялост (НП3). Като наблюдавате графиката и като се има предвид областта на управление на риска (RM), е възможно да забележите три диаграми „пай“, като всяка една съответства на всяко ниво на зрялост Н31, Н32 и Н33. За областта на управление на риска графиката подчертава, че има два елемента, които трябва да бъдат оценени за достигане на първото ниво на зрялост, Н31. В този случай, една оценка „изпълнено в голяма степен“ и една оценка „частично изпълнено“. За второто ниво на зрялост, Н32, моделът предвижда 13 елемента, които трябва да бъдат оценени. Два от тези 13 елемента принадлежат на първо ниво, Н31, а 11 на второто ниво, Н32. Същото се прилага и за третото ниво Н33.

Фигура 7: C2M2 — пример за визуализиране на област



Fully implemented	Цялостно изпълнени
Largely implemented	Изпълнени в голяма степен
Partially implemented	Частично изпълнени
Not implemented	Неизпълнени
MIL1	НП31
MIL2	НП32
MIL3	НП33
RM	RM
ACM	ACM
IAM	IAM
TVM	TVM
SA	SA
ISC	ISC
IR	IR
EDM	EDM
WM	WM
CPM	CPM

Източник: Министерство на енергетиката на САЩ, Служба за доставка и надеждност на електроенергията, 2015 г.

A.3 Рамка за подобряване на киберсигурността на критичната инфраструктура

Рамката за подобряване на киберсигурността на критичната инфраструктура е разработена в рамките на Националния институт по стандарти и технологии (НИСТ). Тя набляга на насочването на дейностите по киберсигурност и управлението на рисковете в рамките на дадена организация. Тя е насочена към всички видове организации, независимо от размера, степента на свързания с киберсигурност риск или усъвършенстването, свързано с киберсигурност. Тъй като това е рамка, а не модел, тя е изградена по различен начин от моделите, анализирани по-рано.

Рамката се състои от три части: ядро на рамката, нива за изпълнение и профили на рамката:

- **Ядрото на рамката**е набор от дейности по киберсигурност, желани резултати и приложими източници, които са общи в секторите на критичните инфраструктури. Те са подобни на атрибутите или измеренията, открити в моделите за зрялост на капацитета за киберсигурност.
- **Нивата за изпълнение на рамката** („нивата“) осигуряват контекст за това как една организация разглежда свързания с киберсигурност риск и действащите процеси за управление на този риск. Като се започне от частично (ниво 1) до адаптивно (ниво 4), нивата описват нарастваща степен на взискателност и изтънченост в практиките за управление на свързания с киберсигурност риск. Нивата не представляват нива на зрялост, а по-скоро те са предназначени да подкрепят организационното вземане на решения за това как да се управлява

свързания с киберсигурност риск, както и кои измерения на организацията са по-висок приоритет и могат да получат допълнителни ресурси.

- **Рамков профил** („профил“) представлява резултатите, основани на нуждите на бизнеса, които една организация е избрала от рамковите категории и подкатегории. Профилът може да се характеризира по отношение на привеждането в съответствие на стандартите, насоките и практиките с ядрото на рамката при конкретен сценарий за изпълнение. Профилите могат да се използват за идентифициране на възможностите за подобряване на положението, свързано с киберсигурността чрез сравняване на „текущ“ профил („настоящо“ състояние) с „целеви“ профил („бъдещо“ състояние).

Ядро на рамката

Ядро на рамката се състои от пет **функции**. Когато се разглеждат заедно, тези функции осигуряват стратегическо виждане на високо ниво на жизнения цикъл на управлението на организация относно свързания с киберсигурност риск. Ядрото на рамката след това идентифицира основните **категории** и **подкатегории** за всяка функция и ги съчетава с примерни информационни източници като съществуващи стандарти, насоки и практики за всяка подкатегория.

Функциите и категориите са подробно описани по-долу:

i **Определяне**: Създаване на организационно разбиране за това как да се управляват рисковете, свързани с киберсигурност за системи, хора, активи, данни, и възможности.
- Подкатегории: управление на активи; бизнес среда; управление; оценка на риска; и стратегия за управление на риска

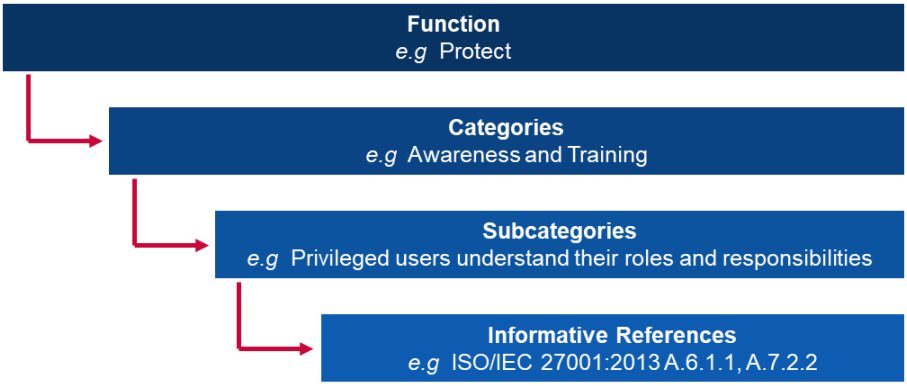
ii **Защита**: Разработване и прилагане на подходящи предпазни мерки за гарантиране на предоставянето на критични услуги.
- Подкатегории: управление на самоличността и контрол на достъпа; осведоменост и обучение; сигурност на данните; процеси и процедури за защита на информацията; поддръжка; и защитни технологии

iii **Откриване**: разработване и изпълнение на подходящи дейности за идентифициране на появата на свързано с киберсигурност събитие.
- Подкатегории: аномалии и събития; продължителен мониторинг на сигурността; и процеси на разкриване.

iv **Отговор**: разработване и изпълнение на подходящи дейности за предприемане на действия във връзка с открит инцидент, свързан с киберсигурност.
- Подкатегории: планиране на отговор; комуникации; анализ; смекчаване и подобрения.

v **Възстановяване**: разработване и изпълнение на подходящи дейности за поддържане на планове за устойчивост и възстановяване на всички способности или услуги, които са били нарушени поради инцидент с киберсигурността.
- Подкатегории: планиране на възстановяването, подобрения; и комуникации

Фигура 8: Пример за рамката за подобряване на киберсигурността на критичната инфраструктура



Function e.g Project	**Функция**напр. проект
Categories e.g Awarness and Training	**Категории** напр. осведоменост и обучение
Subcategories e.g Privileged useres understand their roles and responsibilities	**Подкатегории** напр. привилегированите потребители разбират своите роли и отговорности
Informative References e.g ISO/IEC 27001:2013 A.6.1.1,A.7.2.2	**Информативни източници** напр. ISO/IEC 27001:2013 A.6.1.1,A.7.2.2

Нива

Рамката за подобряване на киберсигурността на критичната инфраструктура се основава на **4 нива**, всяко от които е определено по три оси: Процес на управление на риска, интегрирана програма за управление на риска и външно участие. Нивата не трябва да се считат за нива на зрялост, а като рамка, която предоставя на организациите контекстуализиране на техните виждания относно свързания с киберсигурност риск и съществуващите процеси за управление на този риск.

- **Ниво 1: Частично**
  - **Процес на управление на риска**: организационните практики за управление на свързания с киберсигурност риск не са формализирани, а рискът се управлява ad hoc и понякога по реактивен начин;
  - **Интегрирана програма за управление на риска**: съществува ограничена осведоменост за свързания с киберсигурност риск на организационно ниво. Организацията осъществява управление на риска от киберсигурност нередовно, за всеки отделен случай и не може да има процеси, които позволяват споделянето на информация за киберсигурността в рамките на организацията;
  - **Външно участие**: организацията не разбира ролята си в по-голямата екосистема по отношение на своите зависимости или зависими. Организацията като цяло не е наясно с кибер рисковете за веригата за доставки на продуктите и услугите, които предоставя и които използва;
- **Ниво 2: Информиран риск**
  - **Процес на управление на риска**: практиките за управление на риска се одобряват от ръководството, но не могат да бъдат създадени като организационна политика;
  - **Интегрирана програма за управление на риска**: налице е осведоменост за свързания с киберсигурност риск на организационно равнище, но все още не е създаден организационен подход за управление на свързания с киберсигурност риск. Извършва се оценка на свързания с киберсигурност риск на организационни и външни активи, но обикновено не е повтаряща се или повторна;
  - **Външно участие**: като цяло организацията разбира ролята си в по-голямата екосистема по отношение на собствените си зависимости или зависими, но не и двете. В допълнение, организацията е запозната с кибер рисковете от веригата за доставки, свързани с продуктите и услугите, които предоставя и използва, но не действа последователно или формално по отношение на тези рискове;
- **Ниво 3: Повтарящи се**
  - **Процес на управление на риска**: практиките за управление на риска на организацията са официално одобрени и изразени като политика. Организационните практики за киберсигурност се актуализират редовно въз основа на прилагането на процесите за управление на риска към промени в изискванията за дейността/мисията и променящото се положение, свързано със заплаха и технология;
  - **Интегрирана програма за управление на риска**: съществува организационен подход за управление на свързания с киберсигурност риск. Информираните за риска политики, процеси и процедури се определят, прилагат се по предназначение и се преразглеждат. Висшите ръководители осигуряват разглеждането на киберсигурността чрез всички дейности в организацията;

- **Външно участие**: организацията разбира своята роля, зависимости и зависими в по-голямата екосистема и може да допринесе за по-широкото разбиране на общността за рисковете. Организацията е наясно с кибер рисковете за веригата за доставки на продуктите и услугите, които предоставя и които използва;

- **Ниво 4: Адаптиране**
  - **Процес на управление на риска**: организацията адаптира своите практики за киберсигурност въз основа на предишни и текущи дейности по киберсигурност, включително извлечени поуки и прогнозни показатели;
  - **Интегрирана програма за управление на риска**: съществува организационен подход за управление на риска от киберсигурност, който използва информирани за риска политики, процеси и процедури за справяне с потенциални събития, свързани с киберсигурност; и
  - **Външно участие**: организацията разбира своята роля, зависимости и зависими в по-голямата екосистема и допринася за по-широкото разбиране на общността за рисковете.

Метод на оценка

Рамката за подобряване на киберсигурността на критичната инфраструктура има за цел организациите сами да оценят риска си, за да направят своя подход и инвестиции в киберсигурност по-рационални, ефективни и ценни. За да проучи ефективността на инвестициите, организацията трябва първо да разбере ясно своите организационни цели, връзката между тези цели и подкрепящите резултати за киберсигурността. Резултатите за киберсигурността на ядрото на рамката подкрепят самооценката на инвестиционната ефективност и дейностите по киберсигурност.

A.4 Модел за зрялост на капацитета за киберсигурност на Катар (Q-C2M2)

Моделът на зрялост на капацитета за киберсигурност на Катар (Q-C2M2) е разработен от Колежа по право към Катарския университет през 2018 г. Q-C2M2 се основава на различни съществуващи модели за изграждане на цялостна методология за оценка за подобряване на рамката за киберсигурност на Катар.

Атрибути/Измерения

Q-C2M2 приема подхода на рамката на Националния институт по стандарти и технологии (НИСТ) да използва пет основни функции като основни области на модела. Петте основни функции са приложими в случая с Катар, тъй като те са общи в секторите на критичната инфраструктура, важен елемент в рамката на катарската киберсигурност. Q-C2M2 се основава на **пет области**, всяка област е разделена на няколко **подобласти** за обхващане на целия спектър на зрелостта на възможностите за киберсигурност.

Петте области са подробно описани по-долу:

i **Областта на разбирането** включва четири подобласти: киберуправление, активи, рискове и обучение;
ii Подобластите в рамките на **областта** на **сигурността** включват сигурност на данните, технологична сигурност, сигурност на контрола на достъпа, сигурност на съобщенията и сигурност на персонала;
iii **Областта** на **изложеността** включва подобластите на мониторинга, управлението на инциденти, откриване, анализ и изложеност;
iv **Областта на отговора** включва планиране на отговор, смекчаване и съобщаване на отговора; и
v **Областта на устойчивостта** включва планиране на възстановяването, управление на непрекъснатостта, подобряване, и външни зависимости).

Нива на зрялост

Q-C2M2 използва **5 нива на зрялост**, които измерват зрелостта на възможностите на държавно предприятие или на недържавна организация на ниво основна функция. Тези нива са насочени към оценка на зрелостта в петте области, описани в предишния раздел.

- **Започване**: използва ad hoc практики и процеси за киберсигурност в рамките на някои от областите;
- **Прилагане**: Приети политики за изпълнение на всички дейности по киберсигурност в областите с цел завършване на изпълнението в определен момент;
- **Разработване**: прилагани политики и практики за разработване и подобряване на дейностите по киберсигурност в областите с цел да се предложат нови дейности за изпълнение;
- **Адаптиране**: преразглеждане и преглед на дейности по киберсигурност и приемане на практики, основани на прогнозни показатели, получени от предишен опит и мерки; и
- **Подвижност**: продължаване на използването на адаптивния етап с добавен акцент върху подвижност и скорост при изпълнението на дейности в областите.

Метод на оценка

Q-C2M2 е на ранен етап от научните изследвания и все още не е изграден за изпълнение. Това е рамка, която може да бъде използвана за внедряване на подробен модел за оценка на катарските организации в бъдеще.

A.5 Сертификация на модела за зрялост на киберсигурността (CMMC)

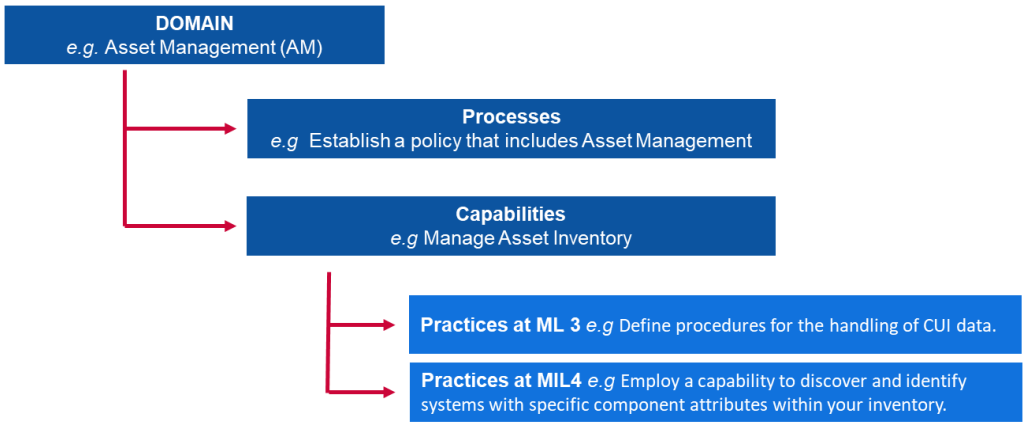
Сертификацията на модела за зрялост на киберсигурността (CMMC) е разработена от Министерството на отбраната (МО) на САЩ в сътрудничество с Университета Карнеги Мелън и лабораторията за приложна физика на Университета „Джон Хопкинс“. Основната цел на МО при създаването на този модел е да защити информацията от сектора на отбранителната промишлена база (ОПБ). Информацията, която CMMC има за цел, е класифицирана или като „информация за федералното споразумение“, информация, предоставена или генерирана от правителството по договор, която не е предназначена за публично оповестяване, или „контролирана некласифицирана информация“, информация, която изисква опазване или контрол на разпространението в съответствие със законите, регламентите и правителствените политики. CMMC измерва зрелостта на киберсигурността и осигурява най-добри практики заедно с елемент на сертифициране за гарантиране на прилагането на практики, свързани с всяко ниво на зрялост. Последната версия на CMMC е пусната през 2020 г.

Атрибути/Измерения

CMMC разглежда **седемнадесет области** , които представляват клъстери от процеси и възможности за киберсигурност. После всяка област се разделя на множество **процеси**, които са сходни в областите; и от една до много **възможности**, които обхващат над пет нива на зрялост. След това възможностите (или възможност) са подробно описани в **практики** за всяко значимо ниво на зрялост.

Връзката между тези понятия е следната:

Фигура 9: Пример на показатели за CMMC



DOMAIN e.g. Asset Management (AM)	**ОБЛАСТ** напр. управление на активи (УА)
Processes e.g Establish a policy that includes Asset Management	**Процеси** напр. създаване на политика, която включва управление на активи
Capabilities e.g Manage Asset Inventory	**Възможности** напр. управление на списъка с активи
Practices at ML 3 e.g Define procedures for the handling of CUI data	**Практики на НПЗ3**напр. Определяне на процедурите за обработка на данни, свързани с КНИ
Practices at MIL4 e.g Employ a capability to discover and identify systems with specific component attributes within inventory	**Практики на НПЗ4**напр. Използване на възможност за разкриване и идентифициране на системи с атрибути на специфичен компонент в рамките на списък

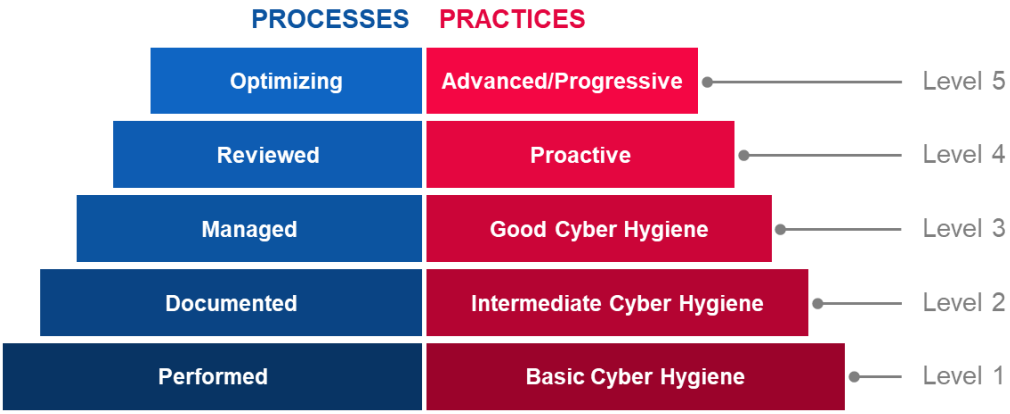
Седемнадесетте области са описани по-долу:

i Контрол на достъпа (КД);
ii Управление на активите (УА);
iii Одит и отчетност (ОО);
iv Осведоменост и обучение (ОО);
v Управление на конфигурацията (УК);
vi Идентификация и удостоверяване (ИУ);
vii Отговор на инцидент (ОИ);
viii Поддръжка (П);
ix Защита на медиите (ЗМ);
x Сигурност на персонала (СП);
xi Физическа защита (ФЗ);
xii Възстановяване (В);
xiii Управление на риска (УР);
xiv Оценка на сигурността (ОС);
xv Информираност за ситуацията (ИС);
xvi Защита на системата и съобщенията (СС);
xvii Интегритет на системата и информацията (СИ).

Нива на зрялост

CMMC използва **5 нива на зрялост** , определени въз основа на процеси и практики. За да достигне определено ниво на зрялост в CMMC, организацията трябва да изпълни предпоставките за процесите и практиките за това ниво. Това също предполага изпълнението на предпоставките на всички нива под това.

Фигура 10: Нива на зрялост на CMMC



PROCESSES	ПРОЦЕСИ
Optimizing	Оптимизиране
Reviewed	Прегледани
Managed	Управлявани
Documented	Документирани
Performed	Изпълнени
PRACTICES	ПРАКТИКИ
Advanced/Progressive	Напреднали/прогресивни
Proactive	Проактивни
Good Cyber Hygiene	Добра кибер хигиена
Intermediate Cyber Hygiene	Средна кибер хигиена
Basic Cyber Hygiene	Основна кибер хигиена
Level 5	Ниво 5
Level 4	Ниво 4
Level 3	Ниво 3
Level 2	Ниво 2
Level 1	Ниво 1

- **Ниво 1**
  - **Процеси — изпълнени**: тъй като организацията може да извършва тези практики само по ad hoc начин и може или не може да разчита на документация. Зрелостта на процеса не се оценява за ниво 1;
  - **Практики — основна кибер хигиена**: ниво 1 набляга на защитата на ИФС (информация за федералното споразумение) и се състои само от практики, които отговарят на основните изисквания за защита;
- **Ниво 2**
  - **Процеси — документирани**: ниво 2 изисква организацията да създаде и документира практики и политики, които да насочват изпълнението на техните усилия за CMMC. Документирането на практиките дава възможност на лицата да ги изпълняват по повторяем начин. Организациите развиват зрели способности чрез документиране на своите процеси и след това ги практикуват, както е документирано;
  - **Практики — средна кибер хигиена**: ниво 2 служи като прогресия от ниво 1 до ниво 3 и се състои от подмножество от изискванията за сигурност, посочени в NIST SP 800—171, както и практики от други стандарти и източници;
- **Ниво 3**
  - **Процеси - управлявани**: ниво 3 изисква организацията да създаде, поддържа и осигури ресурсите за план, който показва управлението на дейностите за изпълнение на практиката. Планът може да включва информация относно мисии, цели, планове за проекти, снабдяване с ресурси, необходимото обучение и участие на съответните заинтересовани страни;

- **Практики — добра кибер хигиена**: ниво 3 набляга на защитата на КНИ и обхваща всички изисквания за сигурност, посочени в NIST SP 800—171, както и допълнителни практики от други стандарти и източници на смекчаване на заплахите;

- **Ниво 4**
  - **Процеси - преразгледани**: ниво 4 изисква организацията да преглежда и измерва практиките за ефективност. В допълнение към измерването на практиките за ефективност, организациите на това ниво могат да предприемат коригиращи действия, когато е необходимо и да информират висшето ръководство за положението или въпросите периодично;
  - **Практики — проактивни**: ниво 4 набляга на защитата на КНИ (контролирана некласифицирана информация) и обхваща подмножество от подобрените изисквания за сигурност. Тези практики подобряват възможностите за откриване и реагиране на дадена организация за справяне и адаптиране към променящите се тактики, техники и процедури;

- **Ниво 5**
  - **Процеси — оптимизиране**: ниво 5 изисква организацията да стандартизира и оптимизира изпълнението на процеса в организацията;
  - **Практики — напреднали/проактивни**: ниво 5 набляга на защитата на КНИ. Допълнителните практики повишават дълбочината и прецизността на възможностите за киберсигурност.

Метод на оценка

CMMC е сравнително млад модел, завършен през първото тримесечие на 2020 г. Досега той не е бил внедрен в нито една организация. Независимо от това, изпълнителите на МО очакват да се свържат със сертифицирани проверяващи трети страни за извършване на одити. МО очаква неговите изпълнители да приложат най-добри практики за насърчаване на киберсигурността и защитата на чувствителната информация.

A.6 Модел за зрялост на киберсигурността на общността (CCSMM)

Моделът на зрялост на киберсигурността на общността (CCSMM) е разработен от Центъра за осигуряване на инфраструктура и сигурност в Тексаския университет. Целта на CCSMM е по-добро определяне на методите за определяне на актуалното състояние на една общност относно нейната кибер подготвеност и осигуряване на пътна карта, която общностите да следват в своите усилия за подготовка. Общностите, които CCSMM цели, са предимно местни или държавни правителства. CCSMM е създаден през 2007 г.

Атрибути/Измерения

Нивата на зрялост се определят съгласно **6 основни измерения** , които обхващат различните аспекти на киберсигурността в общностите и организациите. Тези измерения са ясно определени за всяко ниво на зрялост (подробно посочени на Фигура 311: Резюме на измеренията **за ниво**) 6-те измерения са:

i Насочени заплахи;
ii Показатели;
iii Споделяне на информация;
iv Технология;
v Обучение; и
vi Изпитване.

Нива на зрялост

CCSMM разчита на **5 нива на зрялост** въз основа на основните видове заплахи и дейности, разгледани на ниво:

- **Ниво 1: Осведоменост за сигурността**
  Основната тема на дейностите на това ниво е да запознае хората и

организациите със заплахите, проблемите и въпросите, свързани с киберсигурността;

- **Ниво 2: Развитие на процесите**
  Ниво, предназначено да помогне на общностите да създадат и подобрят процесите за сигурност, необходими за ефективното решаване на въпросите, свързани с киберсигурността;
- **Ниво 3: Позволена информация**
  Създадена да подобри механизмите за споделяне на информация в рамките на общността, за да даде възможност на общността ефективно да корелира на пръв поглед различни видове информация.
- **Ниво 4: Разработване на тактика**
  Елементите от това ниво са предназначени за разработване на по-добри и по-активни методи за разкриване и реагиране на атаки. На това ниво трябва да бъдат осигурени повечето методи за превенция.
- **Ниво 5: Пълен оперативен капацитет за сигурност**
  Това ниво представлява елементите, които трябва да са налице, за да може всяка организация да се счита за напълно оперативно готова да се справи с всякакъв вид кибер заплаха.

Фигура 311: Резюме на измеренията за нивона CCSMM

	Level 1 Security Aware	**Level 2** Process Development	**Level 3** Information Enabled	**Level 4** Tactics Development	**Level 5** Full Security Operational Capability
Threats Addressed	Unstructured	Unstructured	Structured	Structured	Highly Structured
Metrics	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens	Government Industry Citizens
Information Sharing	Information Sharing Committee	Community Security Web Site	Information Correlation Center	State/Fed Correlation	Complete Info Vision
Technology	Rosters, GETS, Access Controls, Encryption	Secure Web Site Firewalls, Backups	Event Correlation SW IDS/IPS	24/7 manned operations	Automated Operations
Training	1-day Community Seminar	Conducting a CCSE	Vulnerability Assessments	Operational Security	Multi-Discipline Red Teaming
Test	Dark Screen - EOC	Community Dark Screen	Operational Dark Screen	Limited Black Demon	Black Demon

Level 1 Security Aware	Ниво 1 Осведоменост за сигурността
Level 2 Process Development	Ниво 2 Разработване на процес
Level 3 Information Enabled	Ниво 3 Позволена информация
Level 4 Tactics Development	Ниво 4 Разработване на тактика
Level 5 Full Security Operational Capability	Ниво 5 Пълен оперативен капацитет за сигурност
Threats Addressed	Насочени заплахи
Metrics	Показатели
Information sharing	Споделяне на информация
Technology	Технология
Training	Обучение
Test	Изпитване
Unstructured	Неструктурирани

Governement Industry Citizens	Правителство Индустрия Граждани
Information Sharing Committee	Комитет за споделяне на информация
Rosters, GETS, Assess Controls, Encryption	Rosters, GETS, контрол на достъпа, криптиране
1-dat Community Seminar	1-дневен семинар на общността
Dark Screen – EOC	Тъмен екран — EOC
Unstructured	Неструктурирани
Governement Industry Citizens	Правителство Индустрия Граждани
Community Security Web site	Уеб сайт за сигурността на общността
Secure Web Site Firewalls, Backups	Сигурни защитни стени на уеб сайт, резервни копия
Conudcting a CCSE	Извършване на CCSE
Community Dark Screen	Тъмен екран за общността
Structured	Структурирани
Governement Industry Citizens	Правителство Индустрия Граждани
Information Correlation Center	Център за корелиране на информация
Event Correlation SW IDS/IPS	Корелация на събитие SW IDS/IPS
Vulnerability Assessment	Оценка на уязвимостта
Operational Dark Screen	Операционен тъмен екран
Structured	Структурирани
Governement Industry Citizens	Правителство Индустрия Граждани
State/Fed Correlation	Корелация държава/фед.
24/7 manned operations	Операции с участие на хора 24/7
Operational Security	Операционна сигурност
Limited Black Demon	Ограничен „черен демон“
Complete Info Vision	Всестранна информационна визия
Highly Structured	Високо структурирани
Automated Operations	Работа в автоматичен режим
Multi-Discipline Red Teaming	Многопрофилно обучение с условни противници (червен екип)
Black Demon	„Черен демон“

Метод на оценка

CCSMM като методология за оценка е предназначен да бъде внедрен от общности с принос от държавни и федерални правоприлагащи органи. Той има за цел да помогне на общността да определи кое е най-важно, кои са най-вероятните цели и какво трябва да бъде защитено (и в каква степен). Като се имат предвид тези цели, могат да бъдат разработени планове, които да приведат всеки аспект на общността до неговото необходимо ниво на зрялост на киберсигурността. Специфичното разузнаване, генерирано от CCSMM помага да се определят целите на различни изпитвания и дейности, които могат да бъдат използвани за измерване на ефективността на създадените програми.

A.7 Модел за зрялост на информационната сигурност за рамката за киберсигурност на НИСТ (ISMM)

Моделът за зрялост на информационната сигурност (ISMM) е разработен в Колежа по компютърни науки и инженерство на Университета „Крал Фахд“ за нефт и минерали в Саудитска Арабия. В него се предлага нов модел на зрелостта на възможностите за измерване на прилагането на мерките за киберсигурност. Целта на ISMM е да даде възможност на организациите да измерват напредъка си по изпълнението във времето, като редовно използват един и същ инструмент за измерване за гарантиране на

запазването на желаното положение, свързано със сигурността. ISMM е разработен през 2017 г.

Атрибути/Измерения

ISMM се основава на съществуващите оценени области на рамката на НИСТ и добавя измерение относно оценката на съответствието. Той свежда модела до **23 оценени области** за положението със сигурността на организация. 23-те оценени области са:

i управление на активи:
ii бизнес среда;
iii управление;
iv оценка на риска;
v стратегия за управление на риска;
vi оценка на съответствието;
vii контрол на достъпа;
viii осведоменост и обучение;
ix сигурност на данните;
x процеси и процедури за защита на информацията;
xi поддръжка;
xii защитна технология;
xiii аномалии и събития;
xiv непрекъснат мониторинг на сигурността;
xv процеси на откриване;
xvi планиране на отговора;
xvii съобщения за отговор;
xviii анализ на отговора;
xix ограничаване на отговора;
xx подобряване на на отговора;
xxi планиране на възстановяването;
xxii подобрения на възстановяването; и
xxiii комуникации за възстановяване.

Нива на зрялост

ISMM разчита на **5 нива на зрялост** , които, за съжаление, не са подробно описани в наличната документация.

- **Ниво 1:** Проведен процес;
- **Ниво 2:** Управляван процес;
- **Ниво 3:** Установен процес;
- **Ниво 4:** Предвидим процес; и
- **Ниво 5:** Процес на оптимизиране.

Метод на оценка

ISMM не предлага конкретна методология за извършване на оценката на организациите.

A.8 Модел за структура за вътрешен одит (IA-CM) за публичния сектор

Моделът за структура за вътрешен одит (IA-CM) е разработен от изследователската фондация на Института за вътрешни одитори с цел изграждане на капацитет и застъпничество чрез самооценка в публичния сектор. Насочен към специалистите по одита, IA-CM предоставя преглед на самия модел заедно с ръководство за прилагане в помощ на използването на модела като инструмент за самооценка.

Въпреки че IA-CM набляга на възможностите за вътрешен одит, а не върху изграждането на капацитет за киберсигурност, моделът е изграден като инструмент за самооценка на зрелостта за субектите от публичния сектор, който може да се прилага в световен мащаб

за подобряване на процесите и ефективността. Тъй като обхватът не е насочен към киберсигурността, атрибутите няма да бъдат анализирани. IA-CM е завършен през 2009 г.

Нива на зрялост

Моделът за структура за вътрешен одит (IA-CM) включва **5 нива на зрялост**, всяко от които описва характеристиките и възможностите на дейността по вътрешен одит на това ниво. Нивата на възможности в модела осигуряват пътна карта за непрекъснато подобрение.

- **Ниво 1: Начало**
  Липсват устойчиви, повтарящи се възможности — зависими от индивидуални усилия
  - Ad hoc или неструктурирани.
  - Изолирани единични одити или прегледи на документи и транзакции за точност и съответствие.
  - Резултатите зависят от уменията на конкретното лице, което заема позицията.
  - Липсват създадени професионални практики, различни от тези, предоставяни от професионални сдружения.
  - Одобрение на финансирането от ръководството, ако е необходимо.
  - Липса на инфраструктура.
  - Одиторите вероятно са част от по-голяма организационна единица.
  - Институционалната способност не е развита.
- **Ниво 2: Инфраструктура**
  Устойчиви и повтарящи се практики и процедури
  - Ключов въпрос или предизвикателство за ниво 2 е как да се създаде и поддържа повторяемост на процесите и по този начин възможност за повтаряне.
  - установяват се отношения за отчитане на вътрешния одит, управленски и административни инфраструктури, както и професионални практики и процеси (насоки, процеси и процедури за вътрешен одит).
  - Планиране на проверката, основано главно на управленски приоритети.
  - Продължаващо разчитане основно на уменията и компетенциите на определени лица.
  - Частично съответствие със стандартите.
- **Ниво 3: Интегрирани**
  управленски и професионални практики, прилагани еднакво
  - Вътрешните одитни политики, процеси и процедури са дефинирани, документирани и интегрирани помежду си и в инфраструктурата на организацията.
  - Управлението на вътрешния одит и професионалните практики са добре установени и се прилагат еднакво в рамките на дейността по вътрешен одит.
  - Вътрешният одит започва да съответства на дейността на организацията и рисковете, пред които е изправена.
  - вътрешният одит се развива от провеждането само на традиционен вътрешен одит до интегриране като отборен играч и предоставяне на съвети относно работата и управлението на рисковете.
  - Фокусът е върху изграждането на екип и капацитета на вътрешната одитна дейност и нейната независимост и обективност.
  - Най-общо отговаря на стандартите.
- **Ниво 4: Управлявани**
  Интегрира информация от цялата организация за подобряване на управлението и управлението на риска
  - Вътрешният одит и очакванията на ключовите заинтересовани страни си съответстват.
  - Въведени са показатели за ефективност за измерване и наблюдение на процесите и резултатите от вътрешния одит.
  - Вътрешният одит е признат, че предоставя значителен принос на организацията.
  - Вътрешният одит функционира като неразделна част от управлението и управлението на риска на организацията.

- Вътрешният одит е добре управлявано бизнес звено.
- Рисковете се измерват и управляват количествено.
- Необходими умения и компетенции са налице с капацитет за подновяване и споделяне на знания (в рамките на вътрешния одит и в организацията).

▶ **Ниво 5: Оптимизиране**

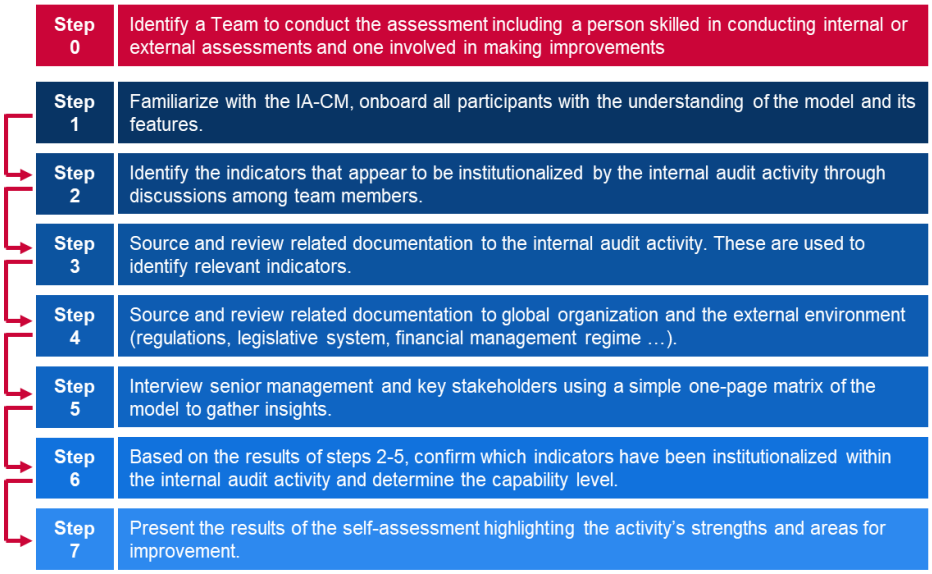
Учене в и извън организацията за непрекъснато усъвършенстване

- Вътрешният одит е образователна организация с непрекъснато усъвършенстване на процесите и иновации.
- Вътрешният одит използва информация в и извън организацията, за да допринесе за постигането на стратегически цели.
- От световна класа/препоръчително/най-добро изпълнение.
- Вътрешният одит е критична част от управленската структура на организацията.
- Професионални и специализирани умения от най-високо ниво.
- Индивидуалните, единичните и организационните мерки за ефективност са напълно интегрирани за
- подобряване на резултатите.

Метод на оценка

Моделът за възможност за вътрешен одит е създаден за самооценка. Той предоставя подробни стъпки, които трябва да следвате за използване на IA-CM и примерна презентация със слайдове за персонализиране. Преди началото на самооценката, даден екип трябва да бъде идентифициран, включително най-малко едно лице, квалифицирано да извършва вътрешни или външни оценки на вътрешния одит и лице, което участва в извършването на подобрения в тази област.

Фигура 12: Стъпки за самооценка на IC-AM



Step 0	Стъпка 0
Step 1	Стъпка 1
Step 2	Стъпка 2
Step 3	Стъпка 3
Step 4	Стъпка 4
Step 5	Стъпка 5
Step 6	Стъпка 6
Step 7	Стъпка 7
Identify a Team to conduct the assessment includiong a person skilled in conducting internal of external assessments and one involved in making improvments.	Посочване на екип за извършване на оценка, включително лице, квалифицирано в провеждането на вътрешни или външни оценки, и лице, което участва в извършването на подобрения.
Familiarize with the IA-CM, onboard all participants with the understanding of the model and its features.	Запознаване с IA-CM, одобряване на всички участници с разбиране на модела и неговите характеристики.

Identify the indicators that appear to be institutionalized by the internal audit activity through discussion among team members.	Идентифициране на показателите, които изглеждат институционализирани от дейността по вътрешен одит чрез обсъждане между членовете на екипа.
Source and review related documentation to the internal audit activity. These are used to identify relevant indicators.	Осигуряване и преглед на свързаната документация за дейността по вътрешен одит. Те се използват за идентифициране на съответните показатели.
Source and review realted documentation to global organisation and the external environment (regulations, legislative system, financial management regime …).	Осигуряване и преглед на свързаната документация за глобалната организация и външната среда (регулации, законодателна система, режим на финансово управление...).
Interview senior management and key stakeholders using a simple one-page matrix of the model to gather insights.	Интервю с висшето ръководство и ключови заинтересовани страни, с използване на проста матрица от една страница на модела за събиране на съвети.
Based on the results of steps 2-5, confirm which indicators have been institutionalized within the internal audit activity and determine the capacity level.	Въз основа на резултатите от стъпки 2—5, потвърждение кои показатели са институционализирани в рамките на дейността по вътрешния одит и определяне на нивото на капацитета.
Present the results of the self-assessment highlighting the activity's strenghts and areas for improvement.	Представяне на резултатите от самооценката, които подчертават силата на дейността и областите за подобрение.

A.9 Глобален индекс за киберсигурност (GCI)

Глобалният индекс за киберсигурност (GCI) е инициатива на Международния съюз по далекосъобщения (МСД), насочена към преразглеждане на ангажимента и ситуацията, свързана с киберсигурността във всички региони на МСД: Африка, Северна и Южна Америка, арабските държави, Азиатско-тихоокеанския басейн, ОНД и Европа, и поставя държавите с висока ангажираност и препоръчителни практики в светлината на прожекторите. Целта на GCI е да помогне на държавите да определят области за подобряване на киберсигурността, както и да ги мотивира да предприемат действия за подобряване на класирането си, като по този начин спомага за повишаване на общото ниво на киберсигурност в световен мащаб.

Тъй като GCI е индекс, а не модел за зрялост, той не използва нива на зрялост, а по-скоро оценка за класиране и сравняване на глобалния ангажимент за киберсигурност на държави и региони.

Атрибути/Измерения

Глобалният индекс за киберсигурност (GCI) се основава на петте стълба на Глобалната програма за киберсигурност (ГПК). Тези стълбове формират петте подиндекса на GCI и всеки от тях включва набор от показатели. Петте стълба и показатели са, както следва:

i **Правен**: мерки, основани на съществуването на правни институции и рамки, които се занимават с киберсигурността и киберпрестъпността.
- Законодателство в областта на киберпрестъпността;
- Регламент за киберсигурност; и
- Ограничаване/контролиране на законодателството за спам.

ii **Технически**: Мерки, основани на съществуването на технически институции и рамки, свързани с киберсигурността.
- CERT/CIRT/ЕРИКС;
- Рамка за прилагане на стандартите;
- Орган по стандартизация;
- Технически механизми и възможности, които са разгърнати в отговор на спама;
- Използване на облак за целите на киберсигурността; и
- Механизми за онлайн закрила на детето.

iii **Организационен**: Мерки, основани на наличието на институции за координация на политиките и стратегии за развитие на киберсигурността на национално ниво.
- Национална стратегия за киберсигурност;
- Отговорна агенция; и
- Киберсигурност.

iv **Изграждане на капацитет**: Мерки, основани на съществуването на научно - изследователска и развойна дейност, програми за образование и обучение,

сертифицирани специалисти и агенции от публичния сектор, които насърчават изграждането на капацитет.
    - Кампании за обществена осведоменост;
    - Рамка за сертифициране и акредитация на професионалисти в киберсигурността;
    - Курсове за професионално обучение по киберсигурност;
    - Образователни програми или академично обучение по киберсигурност;
    - Програми за научно-изследователска и развойна дейност за киберсигурност; и
    - Механизми за стимулиране.
- **Сътрудничество**: Мерки, основани на съществуването на партньорства, рамки за сътрудничество и мрежи за обмен на информация.
    - Двустранни споразумения;
    - Многостранни споразумения;
    - Участие в международни форуми/асоциации;
    - Публично-частни партньорства;
    - Междуведомствени/вътрешноведомствени партньорства; и
    - Най-добри практики.

Метод на оценка

GCI е инструмент за самооценка, изграден чрез проучване[30] на двоични, предварително кодирани и отворени въпроси. Използването на двоични отговори елиминира оценката, основана на мнение и всякакви възможни предразсъдъци към определени видове отговори. Предварително кодираните отговори спестяват време и позволяват по-точен анализ на данните. Нещо повече, простата дихотомна скала позволява по-бърза и по-сложна оценка, тъй като не изисква продължителни отговори, което ускорява и рационализира процеса на предоставяне на отговори и по-нататъшна оценка. Респондентът следва само да потвърди наличието или липсата на някои предварително идентифицирани решения за киберсигурност. Механизъм за онлайн проучване, който се използва за събиране на отговори и качване на съответните материали, дава възможност за извличане на добри практики и набор от тематични качествени оценки от експертна група.

Цялостният процес на GCI се осъществява, както следва:

- До всички участници се изпраща покана, която ги информира за инициативата и с искане за фокусна точка, която отговаря за събирането на всички съответни данни и за попълване на онлайн въпросника на GCI. По време на онлайн проучването одобрената фокусна точка е поканена официално от МСД да отговори на въпросника;
- Събиране на първични данни (за държави, които не отговарят на въпросника):
    - МСД разработва първоначален проект на отговор на въпросника, като използва публично достъпни данни и онлайн проучвания;
    - Проектът на въпросника се изпраща на фокусните точки за преглед;
    - Фокусните точки подобряват точността и след това го връщат;
    - Коригираният проект на въпросника се изпраща до всяка фокусна точка за окончателно одобрение; и
    - Потвърденият въпросник се използва за анализ, оценка и подреждане.
- Вторично събиране на данни (за държави, които отговарят на въпросника):
    - МСД идентифицира липсващите отговори, които подкрепят документи, връзки и т.н.;
    - Фокусната точка подобрява точността на отговорите, когато е необходимо;
    - Коригираният проект на въпросника се изпраща до всяка фокусна точка за окончателно одобрение; и
    - Потвърденият въпросник се използва за анализ, оценка и подреждане.

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

A.10 Индекс на кибер мощността (ИКМ)

Индексът на кибер мощността (ИКМ) е създаден от научно - изследователската програма на Economist Intelligence Unit, спонсорирана от Booz Allen Hamilton през 2011 г. ИКМ е „динамичен количествен и качествен модел, […] който измерва специфични атрибути на кибер средата по четири фактора на кибер мощност: правна и регулаторна рамка; икономически и социален контекст; технологична инфраструктура; и приложение в индустрията, което разглежда цифровия напредък в ключовите индустрии“. Целта на Индекса на кибер мощността е да сравни възможностите на държавите от Г-20 да издържат на кибератаки и да внедрят необходимата цифрова инфраструктура за процъфтяваща и сигурна икономика. Референтният показател, предоставен от ИКМ, поставя акцент върху 19 държави от Г-20 (с изключение на ЕС). След това индексът осигурява класиране на държавите за всеки показател.

Атрибути/Измерения

Индексът на кибер мощността (ИКМ) е базиран на четири фактора на кибер мощност. След това всяка категория се измерва чрез множество показатели, за да се даде конкретна оценка на всяка държава. Категориите и стълбовете са следните:

i **Правна и регулаторна рамка**
- Ангажимент на правителството за кибер развитие
- Политики за киберзащита
- Кибер цензура (или липсата на такава)
- Политическа ефикасност
- Защита на интелектуалната собственост

ii **Икономически и социален контекст**
- Образователни нива
- Технически умения
- Открита търговия
- Степен на иновации в бизнес средата

iii **Технологична инфраструктура**
- Достъп до информационни и комуникационни технологии
- Качество на информационните и комуникационните технологии
- Достъпност на информационните и комуникационните технологии
- Разходи за информационни технологии
- Брой на защитените сървъри

iv **Приложение в промишлеността**
- Интелигентни мрежи
- Електронно здраве
- Електронна търговия
- Интелигентен транспорт
- Електронно управление

Метод на оценка

ИКМ е количествен и качествен модел на оценка. Оценката е извършена от The Economist Intelligence Unit, като се използват количествени показатели от наличните статистически източници и се правят оценки, когато липсват данни. Основните използвани източници са the Economist Intelligence Unit; Организацията за образование, наука и култура на ООН (ЮНЕСКО); Международния съюз по далекосъобщения (МСД)); и Световната банка.

A.11 Индекс на кибер мощността (ИКМ)

Този раздел обобщава основните констатации от анализа на съществуващите модели на зрялост. Таблица5: Преглед на анализираните модели на **зрялост** предоставя преглед на основните характеристики на всеки модел според модифицирания модел на Becker. Таблица 6 Сравняване на нивата на **зрялост** определенията на високо ниво на нивата на зрялост на анализираните модели. Таблица 7 предоставя преглед на измеренията или атрибутите, използвани във всеки модел.

Таблица5: Преглед на анализираните модели на зрялост

Име на модела	Източник на институцията	Цел	Цел	Брой нива	Брой атрибути	Метод на оценка	Представяне на резултатите
Модел за зрялост на капацитета за киберсигурност за държавите (M3K)	Глобален център за капацитет за киберсигурност Оксфордски университет	Увеличаване на мащаба и ефективността на изграждането на капацитет за киберсигурност в международен план	Държави	5	5 основни измерения	Сътрудничество с местната организация за усъвършенстване на модела преди прилагането му в националния контекст	Радар от 5-секции
Модел за зрялост на капацитета за киберсигурност (C2M2)	Министерство на енергетиката на САЩ (ME)	Помага на организациите да оценят и да направят подобрения в своите програми за киберсигурност и да засилят оперативната си устойчивост	Организации от всички сектори, видове и размери	4	10 основни области	Методология за самооценка и инструментариум	Карта за оценка с диаграми „пай“
Рамка за подобряване на киберсигурността на критичната инфраструктура	Национален институт за стандарти и технологии (НИСТ)	Рамка, която цели насочване на дейностите по киберсигурност и управление на рисковете в рамките на организациите	Организации	Без приложение (4 нива)	5 основни функции	Самооценка	-
Модел за зрялост на капацитета за киберсигурност на Катар (Q-C2M2)	Колеж по право към Катарския университет	Осигуряване на работещ модел, който може да се използва за сравнение, измерване и разработване на рамката за киберсигурност на Катар	Катарски организации	5	5 основни области	-	-
Сертификация на модела за зрялост на киберсигурността (CMMC)	Министерство на отбраната на САЩ (МО)	Насърчаване на най-добрите практики, свързани с киберсигурността за защита на информацията	Организации от сектора на отбранителната промишлена база (ОПБ)	5	17 основни области	Оценка от одитори трети страни	-
Модел за зрялост на киберсигурността на общността (CCSMM)	Център за инфраструктурно осигуряване и сигурност, Тексаски университет	Определяне на актуалното състояние на една общност относно нейната кибер подготвеност и осигуряване на пътна карта, която общностите да следват в своите усилия за подготовка	Общности (местни или държавни правителства)	5	6 основни измерения	Оценка в рамките на общностите с принос от държавни и федерални правоприлагащи органи	-
Модел за зрялост на информационната сигурност за рамката за киберсигурност на НИСТ (ISMM)	Колеж по компютърни науки и инженерство Университет „Крал Фахд“ за нефт и минерали, Саудитска Арабия	Позволяване на организациите да измерват своя напредък по изпълнението с течение на времето за гарантиране, че поддържат желаното положение, свързано със сигурността	Организации	5	23 оценени области	-	-
Модел за структура за вътрешен одит (IA-CM) за публичния сектор	Институт на вътрешните одитори, Изследователска фондация	Изграждане на капацитет за вътрешен одит и застъпничество чрез самооценка в публичния сектор	Организации от обществения сектор	5	6 елемента	Самооценка	-
Глобален индекс за киберсигурност (GCI)	Международен съюз по далекосъобщения (МСД)	Преглед на ангажимента и положението в областта на киберсигурността и помощ на	Държави	Без приложение	5 стълба	Самооценка	Таблица за класиране

		държавите да определят области за подобряване на киберсигурността					
Индекс на кибер мощността (ИКМ)	The Economist Intelligence Unit & Booz Allen Hamilton	Да сравни възможностите на държавите от Г-20 да издържат на кибератаки и да внедрят необходимата цифрова инфраструктура за процъфтяваща и сигурна икономика.	Държави от Г-20	Без приложение	4 категории	Сравнителен анализ на the Economist Intelligence Unit	Таблица за класиране

Таблица 6 Сравняване на нивата на зрялост

Модел	Ниво 1	Ниво 2	Ниво 3	Ниво 4	Ниво 5
Модел за зрялост на капацитета за киберсигурност за държавите (M3K)	**Започване** Или не съществува зрялост на киберсигурността, или тя е на много начален етап по естество. Може да има първоначални обсъждания относно изграждането на капацитет за киберсигурност, но не са предприети конкретни действия. Налице е липса на видими доказателства на този етап.	**Формиране** Някои характеристики на аспектите са започнали да растат и да бъдат формулирани, но могат да бъдат ad hoc, дезорганизирани, зле дефинирани или просто „нови“. Доказателствата за тази дейност обаче могат да бъдат ясно показани.	**Създаване** Елементите на аспекта са налице и работят. Няма обаче добре обмислено разглеждане на относителното разпределение на ресурсите. По отношение на „относителните“ инвестиции в различните елементи на аспекта не се взема компромисно решение. Въпреки това, аспектът е функционален и определен.	**Стратегически етап** Направени са избори за това кои части от аспекта са важни и които са по-малко важни за конкретната организация или нация. Стратегическият етап отразява факта, че този избор е направен, в зависимост от обстоятелствата на държавата или организацията.	**Динамичен етап** На този етап съществуват ясни механизми за промяна на стратегията в зависимост от преобладаващите обстоятелства, като например технологията на средата на заплахата, глобалния конфликт или значителна промяна в една област на безпокойство (напр. киберпрестъпност или неприкосновеност на личния живот). Динамичните организации са разработили методи за промяна на стратегиите в ход. Бързото вземане на решения, преразпределянето на ресурсите и постоянното внимание към променящата се среда са характерни за този етап.
Модел за зрялост на капацитета за киберсигурност (C2M2)	**НП30** Практики не се извършват.	**НП31** Извършват се първоначални практики, но могат да бъдат ad hoc.	**НП32** Характеристики на управлението: • Практиките са документирани; • Предоставят се адекватни ресурси в подкрепа на процеса; • Персоналът, който извършва практиките, има адекватни умения и знания; и	**НП33** Характеристики на управлението: • Дейностите се ръководят от политики (или други организационни директиви); • Целите за изпълнение на дейностите по области се определят и наблюдават с цел проследяване на постигнатите резултати; и	-

			• Възлагат се отговорност и права за извършване на практиките. Характеристика на подхода: • Практиките са по-пълни или напреднали отколкото на НП31.	• Документираните практики за дейности на областите са стандартизирани и подобрени в предприятието. Характеристика на подхода: • Практиките са по-пълни или напреднали отколкото на НП32.	
Модел за зрялост на информационната сигурност за рамката за киберсигурност на НИСТ (ISMM)	**Осъществен процес**	**Управляван процес**	**Установен процес**	**Предвидим процес**	**Процес на оптимизиране**
Модел за зрялост на капацитета за киберсигурност на Катар (Q-C2M2)	**Започване** Използва ad hoc практики и процеси за киберсигурност в рамките на някои от областите.	**Разработване** Прилагани политики и практики за разработване и подобряване на дейностите по киберсигурност в областите с цел да се предложат нови дейности за изпълнение.	**Прилагане** Приети политики за изпълнение на всички дейности по киберсигурност в рамките на областите с цел завършване на изпълнението в определен момент.	**Адаптиране** Преразглеждане и преглед на дейности по киберсигурност и приемане на практики, основани на прогнозни показатели, получени от предишен опит и мерки.	**Подвижност** Продължаване на използването на адаптивния етап с добавен акцент върху подвижност и скорост при изпълнението на дейности в областите.
Сертификация на модела за зрялост на киберсигурността (CMMC)	**Процеси: Изпълнени** Тъй като организацията може да извършва тези практики само по ad hoc начин и може или не може да разчита на процеса на документация, зрелостта не се оценява за ниво 1. **Практики: Основна кибер хигиена** Ниво 1 набляга на защитата на ИФС (информация за федералното споразумение) и се състои само от практики, които отговарят на основните изисквания за защита.	**Процеси: Документирани;** Ниво 2 изисква организацията да създаде и документира практики и политики, които да насочват изпълнението на техните усилия за CMMC. Документирането на практиките дава възможност на лицата да ги изпълняват по повторяем начин. Организациите развиват зрели способности чрез документиране на своите процеси и след това ги практикуват, както е документирано; **Практики: Средна кибер хигиена** Ниво 2 служи като прогресия от ниво 1 до ниво 3 и се състои от подмножество от изискванията за сигурност, посочени в НИСТ SP 800—171, както и практики от други стандарти и източници.	**Процеси: Управлявани** Ниво 3 изисква организацията да създаде, поддържа и осигури ресурсите за план, който показва управлението на дейностите за изпълнение на практиката. Планът може да включва информация относно мисии, цели, планове за проекти, снабдяване с ресурси, необходимото обучение и участие на съответните заинтересовани страни. **Практики: Добра кибер хигиена**. Ниво 3 набляга на защитата на КНИ и обхваща всички изисквания за сигурност, посочени в НИСТ SP 800—171, както и допълнителни практики от други стандарти и източници на смекчаване на заплахите.	**Процеси: Прегледани.** Ниво 4 изисква организацията да преглежда и измерва практиките за ефективност. В допълнение към измерването на практиките за ефективност, организациите на това ниво могат да предприемат коригиращи действия, когато е необходимо и да информират висшето ръководство за положението или въпросите периодично. **Практики: Проактивни** Ниво 4 набляга на защитата на КНИ (контролирана некласифицирана информация) и обхваща подмножество от подобрените изисквания за сигурност. Тези практики подобряват възможностите за откриване и реагиране на дадена организация за справяне и адаптиране към	**Процеси: Оптимизиране** Ниво 5 изисква организацията да стандартизира и оптимизира изпълнението на процеса в организацията. **Практики: Напреднали/проактивни** Ниво 5 набляга на защитата на КНИ. Допълнителните практики повишават дълбочината и прецизността на възможностите за киберсигурност.

				променящите се тактики, техники и процедури.	
Модел за зрялост на киберсигурността на общността (CCSMM)	**Осведоменост за сигурността** Основната тема на дейностите на това ниво е лицата и организациите да осъзнаят заплахите, проблемите и въпросите, свързани с киберсигурността	**Развитие на процесите** Ниво, предназначено да помогне на общностите да създадат и подобрят процесите за сигурност, необходими за ефективното решаване на въпросите, свързани с киберсигурността.	**Позволена информация** Създадена да подобри механизмите за споделяне на информация в рамките на общността, за да даде възможност на общността ефективно да корелира на пръв поглед различни видове информация.	**Разработване на тактика** Елементите от това ниво са предназначени за разработване на по-добри и по-активни методи за разкриване и реагиране на атаки. На това ниво трябва да бъдат осигурени повечето методи за превенция.	**Пълен оперативен капацитет за сигурност** Това ниво представлява елементите, които трябва да са налице, за да може всяка организация да се счита за напълно оперативно готова да се справи с всякакъв вид кибер заплаха.
Модел за структура за вътрешен одит (IA-CM) за публичния сектор	**Начало** Липсват устойчиви, повтарящи се възможности — зависими от индивидуални усилия	**Инфраструктура** Устойчиви и повтарящи се практики и процедури	**Интегрирани** Управленските и професионалните практики, прилагани еднакво	**Управлявани** Интегрира информация от цялата организация за подобряване на управлението и управлението на риска	**Оптимизиране** Учене в и извън организацията за непрекъснато усъвършенстване

Таблица 7: Сравнение на атрибути/ измерения

	Модел за зрялост на капацитета за киберсигурност за държавите (M3K)	Модел за зрялост на капацитета за киберсигурност (C2M2)	Модел за зрялост на капацитета за киберсигурност на Катар (Q-C2M2)	Сертификация на модела за зрялост на киберсигурността (CMMC)	Сертификация на модела за зрялост на киберсигурността (CMMC)	Модел за зрялост на информационната сигурност за рамката за киберсигурност на НИСТ (ISMM)	Рамка за подобряване на киберсигурността на критичната инфраструктура	Глобален индекс за киберсигурност (GCI)	Индекс на кибер мощността (ИКМ)
Нива	Пет измерения, разделени на няколко фактора, включително множество аспекти и показатели (Фигура 4)	Десет области, включително уникално управление цел и няколко цели на подхода (Фигура 6)	Пет области, разделени на подобласти	Седемнадесет области, подробно описани в процеси и от една до множество възможности, които след това са подробно изброени в Практики (Фигура 9).	Шест основни измерения	Двадесет и три оценявани области	Пет функции с основни ключови категории и подкатегории (Фигура 8).	Пет стълба, включително няколко показателя	Четири категории с няколко показателя
Атрибути/ Измерения	i Разработване на политика и стратегия за киберсигурност; ii Насърчаване на отговорната култура на киберсигурност в обществото; iii Създаване на знания за киберсигурност; iv Създаване на ефективни правни и регулаторни рамки; и v Контролиране на рисковете чрез стандарти, организации и технологии.	i Управление на риска; ii Управление на активите, промяната и конфигурирането; iii Управление на самоличността и достъпа; iv Управление на заплахите и уязвимостта; v Информираност за ситуацията; vi Реагиране на събития и инциденти; vii Управление на веригата за доставки и на външните зависимости; viii Управление на работната сила; ix Архитектура на киберсигурността; x Управление на програмата за киберсигурност.	i Разбиране (кибер управление, активи, рискове и обучение); ii Сигурност (сигурност на данните, технологична сигурност, сигурност на контрола на достъпа, сигурност на съобщенията и сигурност на персонала); iii Изложеност (мониторинг, управление на инциденти, откриване, анализ и изложеност); iv Отговор (планиране на отговор, смекчаване и съобщаване на отговор); v Поддържане (планиране на възстановяването, управление на непрекъснатостта, подобряване, и външни зависимости).	i Контрол на достъпа; ii Управление на активите; iii Одит и отчетност; iv Осведоменост и обучение; v Управление на конфигурацията; vi Идентификация и удостоверяване; vii Отговор на инцидент; viii Поддръжка; ix Защита на медиите; x Сигурност на персонала; xi Физическа защита; xii Възстановяване; xiii Управление на риска; xiv Оценка на сигурността; xv Информираност за ситуацията; xvi Защита на системата и съобщенията; xvii Интегритет на системата и информацията.	i Насочени заплахи; ii Показатели; iii Споделяне на информация; iv Технология; v Обучение; vi Изпитване.	i Управление на активите; ii Бизнес среда; iii Управление; iv Оценка на риска; v Стратегия за управление на риска; vi Оценка на съответствието; vii Контрол на достъпа; viii Осведоменост и обучение; ix Сигурност на данните; x Процеси и процедури за защита на информацията; xi Поддръжка; xii Защитна технология; xiii Аномалии и събития; xiv Непрекъснат мониторинг на сигурността; xv Процеси на откриване; xvi Планиране на отговора; xvii Съобщения за отговор; xviii Анализ на отговора; xix Ограничаване на отговора; xx Подобряване на на отговора; xxi Планиране на възстановяването; xxii Подобрения на възстановяването; xxiii Комуникации за възстановяване.	i Определяне; ii Защита; iii Откриване; iv Отговор; v Възстановяване.	i Правни; ii Технически; iii Организационни; iv Изграждане на капацитет; v Сътрудничество.	i Правна и регулаторна рамка; ii Икономически и социален контекст; iii Технологична инфраструктура; iv Приложение в промишлеността.

ПРИЛОЖЕНИЕ Б - БИБЛИОГРАФИЯ НА ПРОУЧВАНИЯТА НА БЮРО

Almuhammadi, S. и Alsaleh, M. (2017 г.) „Модел за зрялост на сигурността на информацията за рамката за киберсигурност на НИСТ“, в Computer Science & Information Technology (CS & IT). Шеста международна конференция по конвергенция и услуги в ИТ, Център за сътрудничество в академичните и индустриални изследвания (AIRCC).

Almuhammadi, S. и Alsaleh, M. (2017 г.) „Модел за зрялост на сигурността на информацията за рамката за киберсигурност на НИСТ“, в Computer Science & Information Technology (CS & IT). Достъпно на: https://airccj.org/CSCP/vol7/csit76505.pdf

Anna, S. и колектив (2016 г.) Проверка, анализ и препоръки за защита на критични информационни инфраструктури. Достъпно на: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0415821:EN:HTML

Becker, J., Knackstedt, R. и колектив (2009 г.) Разработване на модели на зрялост за управление на ИТ — процедурен модел и неговото приложение. Достъпно на: https://link.springer.com/content/pdf/10.1007/s12599-009-0044-5.pdf.

Белгийското правителство (2012 г.) „Стратегия за киберсигурност“. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/belgian-cyber-security-strategy/@@download_version/a9d8b992ee7441769e647ea7120d7e67/file_en

Bellasio, J. и колектив (2018 г.) Развитие на капацитет за киберсигурност: ръководство за прилагане на „доказателство за концепцията“. RAND Corporation. Достъпно на: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2000/RR2072/RAND_RR2072.pdf

Bourgue, R. (2012 г.) „Въведение във възвръщаемостта на инвестициите в сигурност“.

Carnegie Mellon University Software Engineering Institute Pittsburgh United States (2019 г.) „Модел за зрялост на капацитета за киберсигурност (C2M2) Версия 2.0. Достъпно на https://apps.dtic.mil/sti/pdfs/AD1078768.pdf

Център за изследване на сигурността (ЦИС), ETH Цюрих (2019 г.) Национални стратегии за киберсигурност в сравнение — предизвикателства за Швейцария. Достъпно на: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-National%20Cybersecurity%20Strategies%20in%20Comparison.pdf

Министерски съвет (2019 г.) Португалски официален вестник, серия 1 — № 108 — Решение на Министерския съвет № 92/2019. Достъпно на: https://cncs.gov.pt/content/files/portugal_-_ncss_2019_2023_en.pdf

Creese, S. (2016 г.) Модел за зрялост на капацитета за киберсигурност за държавите (МЗК). Оксфордски университет.

Зрялост на ЕРИКС — инструмент за самооценка (без дата). Достъпно на: https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey

Проект „CyberCrime@IPA“ на Съвета на Европа и Европейския съюз, Глобален проект за киберпрестъпления на Съвета на Европа и Работна група за киберпрестъпления на Европейския съюз (2011 г.) Специализирани звена за киберпрестъпления — проучване на добрите практики. Достъпно на: https://rm.coe.int/2467-htcu-study-v30-9nov11/16802f6a33

Доклад за свързани с киберсигурността инциденти и система за анализ — инструмент за визуален анализ (без дата). Достъпно на: https://www.enisa.europa.eu/topics/incident-reporting/cybersecurity-incident-report-and-analysis-system-visual-analysis/visual-tool

Darra, E. (2017 г.) Публично-частни партньорства (ПЧП).

Darra, E. (без дата) „Добре дошли в инструмента за обучение за НСКС“.

Dekker, M. A. C. (2014 г.) Технически насоки за докладване на инциденти. Достъпно на: https://resilience.enisa.europa.eu/article-13/guideline-for-incident-reporting/Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf

Dekker, M. A. C. (2014 г.) Технически насоки за мерки за сигурност. Достъпно на: https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf

Dekker, M. A. C. (2015 г.) Насоки за заплахи и активи. Достъпно на: https://resilience.enisa.europa.eu/article-13/guideline_on_threats_and_assets/Guideline_on_Threats_and_Assets_v_1_1.pdf

Digital Slovenia (2016 г.) Стратегия за киберсигурност. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-slovenia

Domingo-Ferrer, J. *и колектив* (2014 г.) *Защита на неприкосновеността на личния живот и данните по план - от политика до инженерство.* Достъпно на: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514111:EN:HTML

Европейската комисия (2012 г.) Регламент на Европейския парламент и на Съвета относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар. Достъпно на: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0238&from=EN

Агенция на Европейския съюз за мрежова и информационна сигурност (2012 г.) НСКС: Практическо ръководство за развитие и изпълнение. Heraklion: ENISA.

Агенция на Европейския съюз за мрежова и информационна сигурност (2012 г.) НСКС: Определяне на курса за национални усилия за укрепване на сигурността в киберпространството. Heraklion: ENISA.

Агенция на Европейския съюз за мрежова и информационна сигурност (2016 г.) Насоки за МСП относно сигурността на обработката на личните данни.

Европейска агенция за мрежова и информационна сигурност (2016 г.) Наръчник за добри практики на НСКС: създаване и прилагане на национални стратегии за киберсигурност. Heraklion: ENISA.

Европейски съюз и Агенция на Европейския съюз за мрежова и информационна сигурност (2017 г.) Наръчник за сигурността на обработката на личните данни. Достъпно на: http://dx.publications.europa.eu/10.2824/569768

Европейски съюз и Агенция на Европейския съюз за мрежова и информационна сигурност (2014 г.) *Описание на CERT на ENISA на екипи и дейности на CERT в Европа*. Достъпно на: http://www.enisa.europa.eu/activities/cert/background/inv/files/inventory-of-cert-activities-in-europe

Изпълнителна служба на Президента (2015 г.) Меморандум за ръководители на изпълнителни отдели и агенции. Достъпно на: https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2016/m-16-04.pdf

Федерално канцлерство на Република Австрия (2013 г.) Австрийска стратегия за киберсигурност. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/austrian-cyber-security-strategy/@@download_version/1573800e2e4448b9bdaead56a590305a/file_en

Федерално министерство на вътрешните работи (2011 г.) Стратегия за киберсигурност за Германия. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/8adc42e23e194488b2981ce41d9de93e/file_en

Ferette, L. (2016 г.) Директива за мрежова и информационна сигурност и национални стандарти за информационна сигурност и неприкосновеност на личния живот за МСП (2015 г.): препоръки за подобряване на приемането на стандарти за информационна сигурност и неприкосновеност на личния живот в малките и средните предприятия. Достъпно на: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ferette, L., Европейски съюз и Европейска агенция за мрежова и информационна сигурност (2015 г.) Докладът за 2015 г. относно националните и международните дейности, свързани с киберсигурност: проучване, анализ и препоръки. Достъпно на: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115948:EN:HTML

Служба на министър-председателя на Франция (2014 г.) Френска национална стратегия за цифрова сигурност. Достъпно на: https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf

Galan Manso, C. и колектив. (2015 г.) Информационна сигурност и неприкосновеност на личния живот за МСП: препоръки за подобряване на приемането на стандарти за информационна сигурност и неприкосновеност на личния живот в малките и средните предприятия. Достъпно на: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0215977:EN:HTML

Ghent University и колектив. (2017 г.) „Оценка на моделите на зрялост на бизнес процесите“, Journal of the Association for Information Systems. Достъпно на: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1775&context=jais

Правителство на България (2015 г.) Национална стратегия за киберсигурност — Кибер-устойчива България 2020 г.

Правителството на Хърватия (2015 г.) Националната стратегия за киберсигурност на Република Хърватия. Достъпно на: https://www.uvns.hr/UserDocsImages/en/dokumenti/Croatian%20National%20Cyber%20Security%20Strategy%20(2015).pdf

Правителство на Гърция (2017 г.) Национална стратегия за киберсигурност. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-greece/view

Правителство на Унгария (2018 г.) Стратегия за сигурност на мрежовите и информационните системи. Достъпно на: https://www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf#!DocumentBrowse

Правителството на Ирландия (2019 г.) Национална стратегия за киберсигурност. Достъпно на: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf

Правителството на Испания (2019 г.) Национална стратегия за киберсигурност. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/the-national-security-strategy/@@download_version/5288044fda714a58b5ca6472a4fd1b28/file_en

Институт на вътрешните одитори (ed.) (2009 г.) Модел за структура за вътрешен одит (IA-CM) за публичния сектор: преглед и ръководство за прилагане. Altamonte Springs, Fla: Институт на вътрешните одитори, Изследователска фондация.

Международен съюз по далекосъобщения (МСД) (2018 г.) Глобален индекс за киберсигурност. Достъпно на: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

Международен съюз по далекосъобщения (МСД) (2018 г.) Ръководство за разработване на национална стратегия за киберсигурност. Достъпно на: https://ccdcoe.org/uploads/2018/10/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

J.D., R. D. B. (2019 г.) „Към модел за зрялост на капацитета за киберсигурност на Катар със законодателна рамка“, International Review of Law.

Правителство на Латвия (2014 г.) Стратегия за киберсигурност на Латвия. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/lv-ncss

Liveri, D. и колектив (2014 г.) Рамка за оценка на националните стратегии за киберсигурност. Heraklion: ENISA. Достъпно на: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0714017:EN:HTML.

Mattioli, R. *и колектив* (2014 г.) *Методологии за идентифициране на активи и услуги от критичната информационна инфраструктура: насоки за картографиране на електронни съобщителни мрежи за данни.* Достъпно на: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0614120:EN:HTML

Министерство на конкурентоспособността и цифровата, морската икономика и икономиката на услугите (2016 г.) Стратегия на Малта за киберсигурност. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-of-malta

Министерство на икономиката и съобщенията (2019 г.) Стратегия за киберсигурност — Република Естония. Достъпно на: https://www.mkm.ee/sites/default/files/kyberturvalisuse_strateegia_2022_eng.pdf

Министерство на националната отбрана на Република Литва (2018 г.) Национална стратегия за киберсигурност

Национален център за киберсигурност (2015 г.) Национална стратегия за киберсигурност на Чешката република. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CzechRepublic_Cyber_Security_Strategy.pdf

Национални стратегии за киберсигурност — Интерактивна карта (без дата). Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map.

Национален инструмент за оценка на стратегиите за киберсигурност (2018 г.) Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/national-cyber-security-strategies-guidelines-tools/national-cyber-security-strategies-evaluation-tool.

Национален институт по стандарти и технологии (2018 г.) Рамка за подобряване на киберсигурността на критичната инфраструктура, Версия 1.1. Gaithersburg, MD: Национален институт за стандарти и технологии Достъпно на: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

Група за управление на обект (2008 г.) Модел за зрялост на бизнес процесите. Достъпно на: https://www.omg.org/spec/BPMM/1.0/PDF

ОИСР, Европейски съюз и Съвместен изследователски център — Европейска комисия (2008 г.) Наръчник за изготвяне на съставни показатели: Методология и ръководство за потребителя. ОИСР. Достъпно на: https://www.oecd.org/sdd/42495745.pdf.

Служба на комисаря по електронните съобщения и пощенските регламенти (2012 г.) Стратегия за киберсигурност на Република Кипър.

Официален вестник на Европейския съюз (2008 г.) Директивата 2008/114/ЕО на Съвета от 8 декември 2008 г. относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита.

Достъпно на: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114&from=EN

Организация за икономическо сътрудничество и развитие (ОИСР) (2012 г.) Изготвяне на политики за киберсигурност в преломен момент. Достъпно на: http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Ouzounis, E. (2012 г.) „Национални стратегии за киберсигурност — практическо ръководство за развитие и изпълнение“.

Ouzounis, E. (2012 г.) Наръчник с добри практики за национални дейности

Portesi, S. (2017 г.) Подобряване на сътрудничеството между ЕРИКС и правоприлагането: Правни и организационни аспекти

Председателство на Министерския съвет (2017 г.) Италианският план за действие за киберсигурност. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-strategic-framework-for-cyberspace-security

Rady Ministrów (2019 г.) Dziennik Urzędowy Rzeczypospolitej Polskiej. Достъпно на: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf

Румънското правителство (2013 г.) Стратегия за киберсигурност на Румъния. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-in-romania

Sarri, A., Kyranoudi, P. и Агенция на Европейския съюз за киберсигурност (2019 г.) Добри практики в областта на иновациите в киберсигурност в рамките на НСКС: добри практики в областта на иновациите в киберсигурност съгласно националните стратегии за киберсигурност. Достъпно на: https://op.europa.eu/publication/manifestation_identifier/PUB_TP0119830ENN.

Секретариат на Комитета за сигурност (2019 г.) Стратегия на Финландия за киберсигурност за 2019 г. Достъпно на: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

Словашкото правителство (2015 г.) Концепция за киберсигурност на Словашката република. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-concept-of-the-slovak-republic

Smith, R. (2015 г.) Директива 2010/41/ЕС на Европейския парламент и на Съвета от 7 юли 2010 г.

Smith, R. (2016 г.) „Директива 2010/41/ЕС на Европейския парламент и на Съвета от 7 юли 2010 г.“ в Smith, R., Основно законодателство на ЕС. London: Macmillan Education. Достъпно на: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0041&from=EN.

Stavropoulos, V. (2017 г.) Европейски месец на киберсигурността за 2017 г.

Шведското правителство (2017 г.) Nationell strategi för samhällets informations- och cybersäkerhet. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/swedish-ncss/view

Датското правителство — Министерство на финансите (2018 г.) Датска стратегия за кибер и информационна сигурност. Достъпно на: https://en.digst.dk/media/17189/danish_cyber_and_information_security_strategy_pdf.pdf

Федерален съвет (2018 г.) Национална стратегия за защита на Швейцария от кибер рискове.

Съвет на правителството на Люксембург (2018 г.) Национална стратегия за киберсигурност. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/strategie-nationale-en-matiere-de-cyber-securite/@@download_version/d4af182d7c6e4545ae751c17fcca9cfe/file_en

Правителство на Нидерландия (2018 г.) Национална програма за киберсигурност. Достъпно на: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en

Белия дом (2018 г.) Национална стратегия за киберсигурност на САЩ. Достъпно на: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

Trimintzios, P. и колектив (2011 г.) Доклад за кибер-Европа. Достъпно на: https://www.enisa.europa.eu/publications/ce2010report

Trimintzios, P., Gavrila, R. и Европейска агенция за мрежова и информационна сигурност (2013 г.) *Оценки на риска на национално ниво: доклад с анализ.* Достъпно на: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0413112:EN:HTML

Trimintzios, P., Gavrila, R., и колектив (2015 г.) Доклад относно сътрудничеството и управлението на кибер кризи. Достъпно на: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0514030:EN:HTML

Trimintzios, P., Ogee, A. и колектив (2015 г.) Доклад относно сътрудничеството и управлението на кибер кризи: общи практики за управление на кризи на ниво ЕС и приложимост към кибер кризи. Достъпно на: http://bookshop.europa.eu/uri?target=EUB:NOTICE:TP0115966:EN:HTML

Национална стратегия за киберсигурност на ОК за периода 2016-2021 г. (2016 г.). Достъпно на: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Университет Инсбрук и колектив (2009 г.) Разбиране на моделите на зрялост.

Wamala, D. F. (2011 г.) „Ръководство за национална стратегия за киберсигурност на МСД. Достъпно на: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

White, G. (2007 г.) „Модел за зрялост на киберсигурността на общността“, през 2007 г. 40-та годишна международна конференция за системните науки в Хавай (HICSS'07)

ПРИЛОЖЕНИЕ В — ДРУГИ ИЗСЛЕДВАНИ ЦЕЛИ

Описаните по-долу цели бяха проучени като част от етапа на проучване на бюро и интервютата, проведени от ENISA. Следните цели не са част от Националната рамка за оценка на възможностите, но те дават информация за теми, които си струва да бъдат обсъдени. Всеки един от следните раздели ще даде обяснение защо целта е била отхвърлена.

- разработване на специфични за сектора стратегии за киберсигурност;
- борба срещу кампаниите за дезинформация;
- Сигурни авангардни технологии (5G, изкуствен интелект, квантови изчисления...);
- гарантиране на суверенитета на данните; и
- Осигуряване на стимули за развитието на индустрията на киберзастраховането.

Разработване на специфични за сектора стратегии за киберсигурност

Приемането на специфични за сектора стратегии, насочени към интервенции и стимули за сектора, със сигурност въвежда по-силен децентрализиран капацитет. То е особено подходящо за държавите членки, чиито ООУ трябва да се занимават с различни рамки и регламенти и където има много зависимости поради секретния характер на киберсигурността. В действителност в няколко държави членки е обичайно да се броят десетки национални органи и регулаторни органи със знание за спецификата на всеки сектор, които имат мандат за прилагане на специфичен регламент за всеки сектор.

Дания, например, започна шест целеви стратегии, насочени към усилията в областта на кибер- и информационната сигурност на най-критичните сектори, за да развие по-силен децентрализиран капацитет в областта на кибер- и информационната сигурност. Всяка „секторна единица“ ще допринесе за оценки на заплахите на секторно равнище, мониторинг, дейностите по подготовка, създаване на системи за сигурност, споделяне на знания и инструкции, наред с другото. Специфичните за сектора стратегии обхващат следните сектори:

- Енергетика;
- Медицински грижи;
- Транспорт;
- Телекомуникации;
- Финанси; и
- Морско дело.

Други държави членки изразиха интерес да разгледат специфични за сектора стратегии за киберсигурност, за да отразят всички регулаторни изисквания. Трябва обаче да се отбележи, че подобна цел може да не отговаря на всички държави членки в зависимост от техния размер, национални политики и зрялост. Голямата трудност да се гарантира, че рамката може да отчита всички специфики, накара ENISA да не включи тази цел в рамката.

Борба срещу кампаниите за дезинформация

Държавите членки интегрират защитата на основните принципи като правата на човека, прозрачността и общественото доверие в своите национални стратегии за киберсигурност. Това е много важно, особено когато става въпрос за дезинформация, която се разпространява чрез традиционните новинарски медии или платформите на социалните медии. Освен това киберсигурността понастоящем е едно от най-големите предизвикателства при изборите. В действителност, дейности като разпространяване на невярна информация или негативна пропаганда са наблюдавани в различни държави в подготовката за важни избори. Тази заплаха има потенциала да подкопае демократичния процес на ЕС. На европейско равнище Комисията очерта план за действие[31] за засилване на усилията за противодействие на дезинформацията в Европа: този план набляга на 4 ключови области (откриване, сътрудничество, сътрудничество с онлайн платформи и осведоменост) и служи за изграждане на възможностите на ЕС и засилване на сътрудничеството между държавите членки.

4 от 19 интервюирани държави изразиха намерението си да се справят с проблема с дезинформацията и пропагандата в своята НСКС.

Например, френската НСКС[32] отбелязва, че: „задължение на държавата е да информира гражданите за рисковете от манипулации и техниките за пропаганда, използвани от злонамерени играчи в интернет. Например, след терористичните атаки срещу Франция през януари 2015 г. правителството създаде информационна платформа за рисковете, свързани с ислямската радикализация чрез електронни съобщителни мрежи: « Stop-djihadisme.gouv.fr ».” Този подход може да бъде разширен, за да отговори на други явления на пропаганда или дестабилизация.

В друг пример НСКС[33] на Полша за периода 2019—2024 г. гласи, че: „срещу манипулативни дейности като кампании за дезинформация, са необходими системни действия за развиване на осведомеността на гражданите в контекста на проверка на автентичността на информацията и реагиране на опитите за изопачаването ѝ“.

Въпреки това по време на интервюта, проведени от ENISA, няколко държави членки споделиха, че не разглеждат въпроса като част от своята НСКС като заплаха за киберсигурността, а по-скоро се занимават с въпроса на по-широко обществено ниво, например чрез инициативи за политика.

[31] https://ec.europa.eu/digital-single-market/en/news/action-plan-against-disinformation
[32] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
[33] http://isap.sejm.gov.pl/isap.nsf/download.xsp/WMP20190001037/O/M20191037.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Сигурни авангардни технологии (5G, изкуствен интелект, квантови изчисления...)

Тъй като значимостта на настоящото положение с кибер заплахата продължава да нараства, развитието на новите технологии най-вероятно ще доведе до увеличаване на интензивността и броя на кибератаките и диверсификацията на методите, средствата и целите, използвани от участниците, свързани със заплахата. Междувременно тези нови технологични решения под формата на авангардни технологии имат потенциала да се превърнат в градивни елементи на европейския цифров пазар. За да се гарантира нарастващата цифрова зависимост на държавите членки и появата на нови технологии, следва да бъдат създадени стимули и пълноправни политики в подкрепа на сигурното и надеждно развитие и внедряване на тези технологии в ЕС.

По време на етапа на проучване на бюро, проведено по отношение на НСКС на държавите членки, бяха представени следните авангардни технологии, които представляват интерес за държавите членки: 5G, изкуствен интелект, квантови изчисления, криптография, периферни изчисления, свързани и автономни превозни средства, големи и умни данни, блокчейн, роботика и интернет на предметите.

По-конкретно, в началото на 2020 г. Европейската комисия публикува съобщение, в което призовава държавите членки да предприемат стъпки за прилагане на набора от мерки, препоръчани в заключенията за инструментите на 5G[34]. Инструментите на 5G са в следствие на Препоръка (ЕС) 2019/534 относно киберсигурността на 5G мрежи, приета от Комисията през 2019 г., която призова за единен европейски подход към сигурността на 5G мрежите[35].

По време на интервюта, проведени от ENISA, беше подчертано, че тази тема е по-скоро тема със секретен характер, която се разглежда в рамките на НСКС, а не като конкретна цел *сама по себе си*.

Гарантиране на суверенитета на данните

От една страна, киберпространството може да се разглежда като страховито глобално общо пространство, което е лесно достъпно, осигуряващо висока степен на свързаност и способно да даде големи възможности за социално-икономически растеж. От друга страна, киберпространството също се характеризира със слабата си юрисдикция, трудност да се приписват действия, липса на граници и взаимосвързани системи, които могат да бъдат „прести“ и чиито данни могат да бъдат откраднати или дори достигнати от чужди правителства. В допълнение към тези две перспективи, цифровата екосистема е белязана от концентрацията на онлайн платформи за услуги и инфраструктура в ръцете на много малко заинтересовани страни. Всички аспекти, посочени по-горе, карат държавите членки да насърчават технологичния суверенитет. Постигането на технологичен суверенитет означава, че гражданите и дружествата могат да съществуват пълноценно чрез използването на цифрови услуги и ИКТ продукти, на които може да се разчита без никакъв страх за личните данни или цифровите активи, икономическата автономия или политическо влияние.

Суверенитетът на данните или технологичният суверенитет се защитава от държавите членки на национално и на европейско ниво. Макар че държавите членки изглежда не разглеждат въпроса директно в своите НСКС като конкретна цел, те или го разглеждат

[34] https://ec.europa.eu/digital-single-market/en/news/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission

[35] https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32019H0534

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

като принцип на секретност, или посочват намерението си да гарантират технологичен суверенитет на национално ниво в *ad hoc* публикации, като наблягат на ключови технологии. Например, във френския стратегически преглед на киберотбраната през 2018 г. се посочва, че „контролирането на следните технологии е от първостепенно значение, за да се гарантира технологичен суверенитет: комуникационно криптиране, откриване на кибератаки, професионално мобилно радио, изчисления в облак и изкуствен интелект“[36].

На европейско ниво държавите членки участват активно в определянето на европейската стратегия за данните (COM/2020/66 final) и в изграждането на рамката на ЕС за сертифициране на цифровите продукти, услугите и процесите от ИКТ сектора, създадена с Акта за киберсигурността на ЕС (2019/881) за гарантиране на стратегическа дигитална автономия на европейско ниво.

Етапът на интервю с държавите членки показа, че темата за технологичния суверенитет често се разглежда като по-широк въпрос от този, който се ограничава до киберсигурността. Ето защо държавите членки не обхващат темата в своите НСКС и за малкото държави, които го правят, те не я покриват като конкретна цел *сама по себе си*.

Осигуряване на стимули за развитието на индустрията на киберзастраховането

Сегашното състояние на индустрията на киберзастраховането показва, че световният пазар безспорно се е увеличил. При все това, той все още е в начален етап, тъй като данните трябва да бъдат събрани и все още трябва да бъдат определени много прецеденти (*напр.* мълчаливо покритие, системни кибер рискове...). Освен това, очакваните загуби, обобщени от кибератаки по целия свят, са няколко степени по-високо от настоящия капацитет за покритие на индустрията на киберзастраховането (Работен документ на МВФ — Киберриск за финансовия сектор: Рамка за количествена оценка WP/18/143). Все пак, развитието на индустрията на киберзастраховането със сигурност може да доведе до ползи и да положи основите на „добродетелни“ механизми. Наистина, механизмите за киберзастраховане могат да помогнат при:

- повишаване на осведомеността относно рисковете от киберсигурност в дружествата;
- количествено оценяване на излагането на кибер рискове;
- подобряване на управлението на риска от киберсигурност;
- предоставяне на подкрепа на организации, които са жертви на кибератаки; и
- покриване на щетите (материални или не), предизвикани от кибератака.

Някои държави членки започнаха да работят по тази тема. Например:

- Естония възприе подход на изчакване и преценка в своята НСКС: „За смекчаване на кибер рисковете в частния сектор като цяло ще бъдат анализирани търсенето и предлагането на киберзастрахователни услуги в Естония и въз основа на това ще бъдат договорени принципи на сътрудничество за свързаните страни, включително споделяне на информация, изготвяне на оценка на риска и т.н. Днес доставчиците на киберзастрахователни услуги са малко на естонския пазар и е необходимо първо да се направи проучване кой какво предлага. Сложността на

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

застрахователната защита често се счита за пречка за развитието на пазара на киберзастраховане“.

- Люксембург специално подкрепя развитието на индустрията на киберзастраховането в своята НСКС: Цел 1: Създаване на нови продукти и услуги. За обединяване на рисковете и насърчаване на жертвите на цифрови кибер инциденти да потърсят помощ от експерти за управление на инцидента и възстановяване на система, засегната от злонамерен акт, застрахователните компании ще бъдат насърчавани да създават специфични продукти в областта на киберзастраховането.“

Обратната връзка от интервюираните беше доста разнообразна по тази тема: някои държави членки заявиха, че темата за киберзастраховането наскоро се превърна в тема на обсъждане, докато други споделиха, че макар темата да е обещаваща, индустрията все още не е достатъчно зряла. Все пак, голям брой интервюирани заявиха, че темата не се разглежда като част от НСКС, или защото тя се счита за твърде специфична или не в рамките на обхвата на НСКС.

TP-02-21-253-BG-N

За Агенцията на Европейския съюз за киберсигурност

Агенцията на Европейския съюз за киберсигурност (ENISA) е агенцията на Съюза, насочена към постигане на високо равнище на киберсигурност в цяла Европа. Създадена през 2004 г. и укрепена с Акта за киберсигурността на ЕС, Агенцията на Европейския съюз за киберсигурност допринася за политиката на ЕС в областта на киберсигурността, повишава надеждността на ИКТ продукти, услуги и процеси със схеми за сертифициране на киберсигурността, сътрудничи си с държавите членки и органите на ЕС и помага на Европа да се подготви за бъдещи предизвикателства в областта на киберсигурността. Агенцията работи съвместно с ключовите си партньори — чрез обмен на знания, изграждане на капацитет и повишаване на осведомеността — за повишаване на доверието в свързаната с интернет икономика, за стимулиране на устойчивостта на инфраструктурата на Съюза и в крайна сметка за гарантиране на цифровата сигурност на обществото и гражданите на Европа. За повече информация вж. www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

Heraklion office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN: 978-92-9204-475-6
DOI: 10.2824/558701