IT4Sec Reports 138
http://dx.doi.org/10.11610/it4sec.0138

Сравнителен анализ на модели за оценяване на зрелостта на способностите за киберсигурност

Венелин Георгиев

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, май 2021

Венелин Георгиев, Сравнителен анализ на модели за оценяване на зрелостта на способностите за киберсигурност, *IT4Sec Reports 138* (май 2021), http://dx.doi.org/10.11610/it4sec.0138

IT4Sec Reports 138 „Сравнителен анализ на модели за оценяване на зрелостта на способностите за киберсигурност“ Всичко онова, което се прави в областта на киберсигурността, киберустойчивостта и противодействието срещу киберпрестъпността може да бъде фокусирано върху един термин и това е терминът способности за киберсигурност. Способностите за киберсигурност демонстрират възможностите за изпълнение на политики, стандарти, указания и оперативни процедури за сигурност на информационни системи, мрежи, приложения и информация. От своя страна способностите за киберсигурност представляват динамичен обект, който се изгражда, поддържа, развива, модифицира и адаптира към променящата се среда за сигурност. Динамиката при способностите за сигурност налага измерване на степента на тяхната зрялост и съпоставяне с целевите нива. В доклада се прави сравнителен анализ на съществуващи модели за оценяване на зрелостта на способностите за киберсигурност като по този начин се създава възможност за аргументиран избор на подобен метод за нуждите на конкретно оценяване.

Ключови думи: способности, киберсигурност, киберустойчивост, нива на зрялост, области за киберсигурност, модели за измерване на зрелостта на способностите за киберсигурност

IT4SecReports 138 „Comparative Analysis of Models for Assessing the Maturity of Cybersecurity Capabilities“ The examination of all issues of interest in the field of cybersecurity, cyber resilience and the fight against cybercrime can be focused on one term, and that is the term cybersecurity capabilities. Cybersecurity capabilities demonstrate the ability to implement policies, standards, guidelines, and operational procedures for the security of information systems, networks, applications, and information. In turn, cybersecurity capabilities are a dynamic object that is built, maintained, developed, modified and adapted to the changing security environment. The dynamics of security capabilities require measuring the degree of their maturity and comparing them with the target levels. This report provides a comparative analysis of existing models for assessing the maturity of cybersecurity capabilities, thus creating an opportunity for a reasonable choice of such a method for the needs of specific assessment.

Keywords: capabilities, cybersecurity, cyber resilience, maturity level, cybersecurity areas, measurement, assessment

ISSN 1314-5614

Ако във фокуса на едно изследване бъдат поставени способностите за киберсигурност няма да бъде трудно да бъдат намерени подходящи аргументи за обосноваване на значимостта и актуалността на това изследване. Като примери за подобни аргументи могат да бъдат посочени:

- непрекъснатото нарастване на обхвата и мащаба на приложение на информационни технологии в бизнеса, държавното управление и личния живот на гражданите;
- появата на нови и модифицирани заплахи за сигурността на информационните системи, мрежи, приложения и информация;
- огромните щети, финансови и нефинансови, които потребителите в лицето на фирмите, държавните институции и индивидуалните потребители понасят в следствие на кибератаки и киберпрестъпления и т.н.

Способностите за киберсигурност представляват динамичен обект, чието управление изисква възможности за измерване на нивото на тяхната зрялост и сравняване на оперативните стойности с предварително определени целеви стойности (най-често в националните стратегии за киберсигурност). За нуждите на измерването нивото на зрялост на способностите за киберсигурност е необходим модел, който да бъде адекватен на обекта, чийто способности се измерват. В общия случай като такива обекти могат да бъдат определени отделни фирми или държавите като цяло.

Измерването на степента на зрялост на способностите за киберсигурност може да бъде направено с помощта на вече съществуващ модел или с помощта на специално разработен модел. Сравнителният анализ на съществуващите модели за измерване на зрелостта на способностите за киберсигурност подпомага потребителите при избора на подходящ модел или чрез посочване на добри практики в случай на разработване на нов модел.

На базата на горните аргументи е извършен сравнителен анализ на модели за измерване на зрелостта на способностите за киберсигурност. В рамките на изследването са сравнени следните модели:

- Cybersecurity Capabilities Maturity Model (C2M2) – M1 [1]
- National Capabilities Assessment Framework (NCAF) – M2 [2]
- Cybersecurity Capacity Maturity Model for Nations (CCMM) – M3 [3]
- Framework for Improving Critical Infrastructure Cyber Security (FICICS) – M4 [4]
- Qatar Cybersecurity Capability Maturity Model (Q-C2M2) – M5 [5]
- Cybersecurity Maturity Model Certification (CMMC) – M6 [6]
- The Community Cyber Security Maturity Model (CCSMM) – M7 [7]
- Information Security Maturity Model for NIST Cyber Security Framework (ISMM) – M8 [8]

[1] “National Capabilities Assessment Framework,” European Union Agency for Cybersecurity (ENISA), 2020.

[2] Пак там

[3] Global Cyber Security Capacity Centre, University of Oxford, *Cybersecurity Capacity Maturity Model for Nations (CMM)*, 2016.

[4] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.1., 2018, Gaithersburg. Available at: http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[5] “National Capabilities Assessment Framework.”

[6] Пак там

[7] Gregory White, ‘The Community Cyber Security Maturity Model’, in 40th Hawaii International International Conference on Systems Science (HICSS-40 2007), 3-6 January 2007, Waikoloa, Big Island, HI, USA.

[8] “National Capabilities Assessment Framework.”

- The Global Cybersecurity Index (GCI) – M9 [9]
- The Cyber Power Index (CPI) – M10 [10].

С цел опростяване използването на отделните модели в хода на сравнението, на същите са присвоени съответните кодове, състоящи се от буквата М и съответен цифров индекс (кодовете са посочени по-горе, при изброяване на самите модели).

Критериите, на базата на които е извършено сравнението, са следните:

- организация, която е разработила модела;
- ниво на способностите за киберсигурност, за което се отнася модела;
- цели и предназначение на модела;
- структуриране на областите в полето на киберсигурността;
- използвани нива на зрялост.

Допускания, направени преди извършване на сравнението:

- различните модели са базирани на различни нива на научна обоснованост и осигуреност;
- различна е степента на свързаност и взаимно влияние между отделните компоненти на моделите;
- за различните модели може да бъде намерена информация с различна степен на детайлност;
- изборът на модели, включени в сравнителния анализ, е направен на базата на художествена абстракция.

1. Организация, която е разработила модела

M1 – Моделът е разработен от U.S. Department of Energy (DOE).

M2 – Моделът е разработен от European Union Agency for Cybersecurity (ENISA) през 2012 г.

M3 - Моделът е разработен от Global Cyber Security Capacity Centre, който е част от Оксфордския университет. Първоначално моделът е разработен през 2014 г., като през 2016 г. е обновен на базата на препоръките от единадесет държави, които са го прилагали.

M4 - Рамката е разработена от NIST и е предназначена да насочва дейностите в областта на киберсигурността и управление на риска в организациите.

M5 - Моделът е разработен от Qatar University's College of Law през 2018 г. Базира се на различни съществуващи модели за оценяване и повишаване на способностите за киберсигурност.

M6 - Моделът е разработен в министерство на отбраната на САЩ в сътрудничество с Carnegie Mellon University Johns Hopkins University Applied Physics Laboratory.

M7 - Моделът е разработен от Centre for Infrastructure Assurance and Security заедно с The University of Texas през 2007 г.

M8 - Моделът е разработен в университет в Саудитска арабия през 2017 г.

M9 - Инициативата за разработване на индекса е на International Telecommunication Union.

[9] International Telecommunication Union (ITU), "The Global Cybersecurity Index," 2018, Available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[10] "National Capabilities Assessment Framework."

М10 - Индексът е разработен по програма на Economist Intelligence Unit през 2011 г.

2. Ниво на способностите за киберсигурност, за което се отнася модела

М1 – Моделът е адресиран към оценяване на зрелостта на способностите за киберсигурност на организации от всякакъв вид, сектор и мащаб.

М2 – Моделът е разработен с цел създаване на възможности за измерване зрелостта на способностите за киберсигурност на ниво държава.

М3 – Моделът е адресиран към измерване на зрелостта на способностите за киберсигурност на ниво държава.

М4 – Моделът може да бъде прилагана за оценяване на зрелостта на способностите за киберсигурност за организации от всякакъв тип, независимо от мащаба на техния бизнес, вида на рисковете и спецификите на киберсредата и киберсигурността.

М5 – Моделът е адресиран към измерване на зрелостта на способностите за киберсигурност на ниво държава.

М6 – Моделът е адресиран към измерване на зрелостта на способностите за киберсигурност на отбранителната индустриална база.

М7 – Моделът е адресиран към измерване на зрелостта на способностите за киберсигурност на отделните държави.

М8 – Моделът е приложим при измерване на зрелостта на способностите за киберсигурност на ниво организация.

М9 – Моделът е приложим при измерване на способностите за киберсигурност на ниво отделна държава.

М10 – Моделът е приложим за определяне на нивото на способностите за киберсигурност на отделна държава.

3. Цели и предназначение на модела

М1 – Целта на модела е да подпомогне организациите при оценяване и развитие на техните програми за киберсигурност и повишаване на тяхната оперативна устойчивост.

М2 – Целта на разработването на модела е да се предостави инструмент за самооценяване нивото на зрялост на способностите за киберсигурност на страните от Европейския съюз, на базата на техните национални стратегии за киберсигурност. Идеята е по този начин да се повиши ефективността на усилията за създаване и развитие на способности за киберсигурност както на стратегическо, така и на оперативно ниво.

М3 - Целта на модела е да се повиши ефективността на процеса за изграждане на способности за киберсигурност на страната.

М4 - Целта на модела е да подпомага организациите при ръководството на дейностите в полето на киберсигурността и управлението на риска.

М5 – Целта на модела е да се осигури приложим инструмент, който може да използва бенчмарк концепцията при измерване и развитие на киберсигурността на Катар.

М6 - Основната цел на модела е оценяване на степента на защита за информацията на отбранителната индустриална база.

М7 – Целта при създаване на модела е подобряване на възможностите за оценяване и развитие на способностите за киберсигурност чрез създаване на пътна карта за усилията в тази област.

М8 – Целта при разработване на модела е създаване на възможност за оценяване на способностите за киберсигурност на организацията.

М9 – Целта пред модела е създаване на възможности за преглед и оценяване на ангажиментите в областта на киберсигурността на страните от Африка, Америка, арабските страни, Тихоокеанския регион на Азия и Европа.

М10 – Моделът е предназначен за извършване на динамична количествена и качествена оценка на специфични характеристики на киберсредата и киберспособностите.

4. Структуриране на областите в полето на киберсигурността, в които се оценява зрелостта на способностите за киберсигурност

М1 – Способностите за киберсигурност, които се оценяват, са структурирани в десет области. Всяка област има уникални цели на стратегическо и оперативно ниво. Десетте области включват: управление на риска; мениджмънт на активите, промените и конфигурацията; мениджмънт на идентичността и достъпа; мениджмънт на заплахите и уязвимостите; ситуационна готовност; отговор на инциденти и събития с киберсигурността; мениджмънт на веригите за доставка и външна зависимост; мениджмънт на персонала; архитектура за киберсигурност; мениджмънт на програмата за киберсигурност.

М2 – Моделът оценява зрелостта на способностите за киберсигурност в четири области: ръководство и стандарти за киберсигурност (измерват се способностите на страната да изграждат адекватно ръководство, стандарти и добри практики в областта на киберсигурността; отчитат се различни аспекти на киберустойчивостта и киберотбраната); капацитет за изграждане на способности за киберсигурност и осведоменост на потребителите (оценяват се способностите на страната да повишава информираността на потребителите за заплахите и рисковете пред киберсигурността, а също така как да се противодейства срещу тях; оценяват се също така и възможностите на страната да изгражда способности за киберсигурност и за провеждане на научни изследвания в областта); закони и регулации (измерват се способностите на страните да прилагат закони и регулации в отговор на растящата киберпрестъпност и нарастващия брой киберинциденти, както и за защита на обектите от критичната инфраструктура); кооперииране и сътрудничество (оценява се степента за сътрудничество и обмен на информация между страните и заинтересованите групи лица; формите за сътрудничество се разглеждат като инструменти за подобряване на базирането и даване на отговор на промените в заплахите, идващи от средата). В рамките на изброените по-горе четири области, в модела се определят и съответните цели (общо 17 на брой).

М3 - В модела са включени и се отчитат пет области в полето на киберсигурността. Във всяка област има фактори, с помощта на които се описват детайлите от изграждането на способности за киберсигурност. За всеки фактор се дефинират аспекти, конкретизиращи обхвата на фактора. Аспектите помагат при формулиране на подобласти с по-малък обхват. Всеки аспект се оценява с помощта на метрики/индикатори, описващи стъпките, действията и състоянията, които са включени в съответното ниво на зрялост. Петте области в полето на киберсигурността, които се отчитат в модела са: създаване на политика и стратегия за киберсигурност, в която се съдържат шест фактора; повишаване на организационната култура за киберсигурност в обществото, в която се съдържат пет фактори; разширяване на обема от знания в областта на киберсигурността, в която са включени три фактора; създаване на достатъчно ефективна законова и регулационна рамка в сферата на киберсигурността, в която се съдържат три фактора; управление на риска за киберсигурността, в която се съдържат седем фактора.

М4 – В модела се използват пет области (функции), които отчитани заедно осигуряват стратегическата гледна точка към жизнения цикъл за мениджмънт на риска за киберсигурността в организацията. На следващо място има категории и подкатегории за всяка от областите като се търси съответствие със стандарти, ръководства и добри практики. Петте области от модела са: идентифициране на риска за киберсигурността; защита на активите; разкриване на инциденти с киберсигурността; отговор на инцидент с киберсигурността; възстановяване след инцидент с киберсигурността.

М5 - Моделът адаптира модела на NIST за използване на пет ключови функции като основни области в полето на киберсигурността. Всяка от петте области включва подобласти, които изчерпват обхвата на способностите за киберсигурност, чиято зрялост се измерва. Петте области и включените в тях подобласти са: „Разбиране“; „Сигурност“; „Излагане на риск“; „Отговор“; „Устойчивост“.

М6 - Моделът отчита седемнадесет области, представляващи клъстери в процесите и способностите за киберсигурност. Всяка от областите включва процеси и способности, оценявани в рамките на пет нива за зрялост. Способностите за киберсигурност са детайлизирани в практики, които също съответстват на нивата на зрялост. Самите области могат да бъдат описани по следния начин: контрол на достъпа; мениджмънт на активите; отчетност и одитиране; информираност и подготовка на потребителите; мениджмънт на конфигурирането; идентифициране и автентификация; отговор на инциденти с киберсигурността; поддържане на сигурна среда; защита на медиите; персонална сигурност; физическа сигурност; възстановяване след инцидент с киберсигурността; управление на риска за киберсигурността; оценяване на сигурността на данните; ситуационна готовност; защита на системите и комуникациите; интегритет на системите и информацията.

М7 – Моделът използва шест области, осигуряващи различен аспект на киберсигурността. Областите са: заплахи за киберсигурността; метрики за киберсигурност; споделяне на информация; технологии; обучение на потребителите; тестване на състоянието на киберсигурността.

М8 - Моделът използва областите на киберсигурността, посочени в модела на NIST като допълва тези области с една нова – оценяване на съответствието.

М9 - Моделът „стъпва“ върху петте колони (области) от Global Cybersecurity Agenda. Тези колони формират пет подиндекса, като всеки от тях включва специфични индикатори, отнасящи се до киберсигурността и киберпрестъпността. Областите могат да бъдат описани по следния начин: „Нормативна“, „Техническа“, „Организационна“, „Изграждане на капацитет“, „Кооперирание в областта на киберсигурността“.

М10 - В индекса се използват четири драйвъра (области) за киберсигурност и кибермощ като всеки от тях се измерва с помощта на индикатори. Областите са: „Законова и регулаторна рамка“; „Икономически и социален контекст“; „Технологична инфраструктура“; „Приложение в индустрията“.

5. Използвани в модела нива на зрялост за оценяване на способностите за киберсигурност

М1 – В модела се използват четири нива на зрялост на способностите за киберсигурност. Ниво 0: Не се прилагат процедури за киберсигурност. Ниво 1: Прилагат се първоначални процедури за киберсигурност, но това става ad-hoc. Ниво 3: Прилаганите практики за киберсигурност са документирани и осигурени с ресурси; персоналът, изпълняващ процедурите е подготвен и разполага с нужните умения; разпределени са ролите и отговорностите за изпълнение на процедурите. Ниво 4: Практиките се определят

на базата на политики и стандарти за киберсигурност, които редовно се преглеждат и обновяват.

М2 – В модела се използват пет нива на зрялост, които следват процеса за изграждане и развитие на способностите за киберсигурност, т.е. те представят нарастващи нива на зрялост. Нивата надграждат оценките на зрелостта на способностите за киберсигурност от ниво 1: страната няма ясен подход за изграждане и оценяване на способностите за киберсигурност (възможно е да съществуват някакви цели, които са описани прекалено общо; възможно е също така да се провеждат епизодични изследвания в областта на способностите за киберсигурност), до ниво 5: националната стратегия за изграждане на способности за киберсигурност е динамична и адаптивна към промените в средата (заплахи, нови технологии, мащабни кибер конфликти и т.н.). Добиваната информация се използва при взимане на решения за развитие на способностите за киберсигурност. Налице са възможности за бързо подобрение на текущото ниво на способности за киберсигурност.

М3 - Моделът използва пет нива на зрялост: начално или стартово ниво (на това ниво не съществуват способности за киберсигурност или има някакви, но тяхното ниво на зрялост е изключително ниско); формиращо (в някои области се появяват способности, но те се създават ad-hoc, неорганизирано и са неясно дефинирани); изграждащо (отделни компоненти на способностите за киберсигурност са налице и се прилагат. Няма достатъчна рационалност при разпределение на ресурсите); стратегическо (приоритизират областите в полето на киберсигурността, както и аспектите, отчитани в модела); динамично (съществуват механизми за преглед на областите и аспектите, отчитани в модела, във връзка с промени в средата. Съществува достатъчно бърз процес за взимане на решения и разпределяне на ресурсите за нуждите на способностите за киберсигурност).

М4 - Моделът използва четири нива на зрялост (изпълнителни вериги), всяко от които се определя с помощта на три компонента: процес за управление на риска; интегрирана програма за управление на риска; външно участие. Описанието на тези вериги може да бъде направено по следния начин: първо ниво „Частично“ (организацията не разполага с формализирани процедури и практики за управление на риска за киберсигурността; рискът се управлява ad-hoc като често пъти се прилага реактивен подход; в организацията има ограничена осведоменост за рисковете за киберсигурността; управлението на риска не е редовна дейност, а се извършва само при възникване на конкретен случай като информация за управлението на риска не се споделя в организацията; организацията не разбира своята роля в една по-широка екосистема както като зависима страна, така и като оказваща влияние страна; организацията по-често не е подготвена за киберрисковете идващи от продуктите за доставка на продукти и услуги, които тя доставя и които получава); второ ниво „Информиран риск“ (процедурите за управление на риска в организацията са утвърдени от стратегическия мениджмънт, но не са обединени в организационна политика; в организацията съществува осведоменост относно рисковете за киберсигурността, но не съществува достатъчно изчерпателен подход за управление на тези рискове; оценката на риска за киберсигурността на организацията не се извършва редовно/регулярно; организацията разбира своята роля в една по-широка екосистема по отношение на своята зависимост, както и по отношение на влиянието, което оказва; организацията обръща внимание на киберриска, свързан с веригите за доставка, но не работи официално върху тези рискове); трето ниво „Повторимо“(практиките за управление на риска за киберсигурността на организацията са обединени в съответна политика; тези практики редовно се преглеждат и обновяват на базата на текущи промени в бизнеса, технологиите и външната среда; организацията прилага изчерпателен подход за управление на риска за киберсигурността; дефинирани,

прилагани и усъвършенствани са политиките, процесите и процедурите за управление на риска за киберсигурността; организацията разбира своята роля като част от една по-широка екосистема и допринася за общото разбиране на рисковете за киберсигурността); четвърто ниво „Адаптивно“ (организацията адаптира практиките си в областта на киберсигурността на базата на резултати от минали и текущи дейности, поуки от практиката, използване на метрики и индикатори; организацията прилага изчерпателен подход за управление на риска за киберсигурността при използване на политики, процеси и процедури, информирани по отношение на риска за да отговаря на потенциални събития, свързани с киберсигурността; организацията разбира своето място и роля в една по-широка екосистема и допринася за по-широкото разбиране на риска за киберсигурността).

М5 - В модела се използват пет нива на зрялост, с помощта на които се измерва нивото на зрялост на способностите за киберсигурност на публични и частни организации на ниво функции. Описанието на нивата на зрялост може да бъде направено по следния начин: първо ниво „Инициииране“ (в рамките на това ниво се прилагат ad-hoc процедури и практики за киберсигурност в съответната област); второ ниво „Изпълнение“ (прилагат се адаптирани политики за изпълнение на дейностите от сферата на киберсигурността във всяка от областите, като се търси допълване с нови дейности); трето ниво „Развитие“ (прилагат се политики за подобряване и развитие на дейностите в полето на киберсигурността във всяка от областите); четвърто ниво „Адаптиране“ (извършва се преглед на дейностите в полето на киберсигурността и одобряване на нови практики на базата на предвиждащи индикатори от предишни изследвания и обучения); пето ниво „Гъвкавост“ (осигуряване на динамичност на дейностите в полето на киберсигурността при прилагането им в различните области).

М6 – В модела се използват пет нива на зрялост, определени на базата на процесите и практиките в сферата за киберсигурност. Признаването на всяко от нивата за зрялост изисква изпълнението на съответните процеси и практики, както и на процесите и практиките от предходните нива. Описанието на нивата за зрялост може да бъде направено по следния начин: първо ниво „Изпълнение“(организацията изпълнява практиките за киберсигурност ad-hoc без да ги документира; практиките са фокусирани върху защитата на информацията и отговарят на базови изисквания за сигурност); второ ниво „Документиране“ (в организацията съществуват документирани политики и практики, които ръководят усилията в полето на киберсигурността; документирането на практиките помага те да бъдат изпълнявани по един и същи начин от различни лица; документирането на практиките се разглежда като част от процеса за изграждане на способности за киберсигурност; прилаганите практики в полето на киберсигурността отговарят на изискванията от NIST SP800-171, както и на изискванията от други стандарти); трето ниво „Управление“ (организацията разработва, прилага и осигурява ресурси за план, по който се изграждат способности за киберсигурност; практиките се фокусират върху защитата на информацията и включват изискванията от NIST SP 800-171, както и то други стандарти); четвърто ниво „Контролиране“ (организацията преглежда и измерва ефективността на практиките като на тази база се взимат коригиращи решения; практиките се фокусират върху защитата на информацията и включват съвкупност от изисквания за сигурност; насочени са към създаване на способности за киберсигурност, които са адекватни на заплахите от средата); пето ниво „Оптимизиране“ (организацията стандартизира и оптимизира процесите по изграждане на способности за киберсигурност; практиките са фокусирани върху защитата на информацията; с помощта на допълнителни практики се увеличава дълбочината и комплексността на способностите за киберсигурност).

М7 - Моделът използва пет нива на зрялост, определяни на базата на вида на заплахите и съответните дейности. Описание на нивата на зрялост може да бъде

направено по следния начин: първо ниво „Осведоменост“ (организациите и потребителите са информирани за заплахите, проблемите и решенията, свързани с киберсигурността); второ ниво „Разработване на процес“ (създаване и непрекъснато подобряване на процес, който да отговаря на проблемите с киберсигурността); трето ниво „Споделяне на информация“ (в организацията се обръща специално внимание за подобряване на възможностите за споделяне на информация по сигурен начин); четвърто ниво „Разработване на тактики“ (в организацията се разработват проактивни методи (включително превантивни методи) за откриване и отговор на кибератаки); пето ниво „Пълен комплект от оперативни способности за киберсигурност“ (организацията има пълна оперативна готовност за отговор на заплахите за киберсигурността).

М8 - В модела се използват пет нива за оценяване на зрелостта на способностите за киберсигурност, които не са детайлизирани. Нивата могат да бъдат определени като: изпълняван процес; управляван процес; изграден процес; предсказуем процес; оптимизиран процес за изграждане на способности за киберсигурност.

М9 - Индексът не е модел за оценяване на нивото на зрялост на способностите за киберсигурност и по тази причина в него не се използват нива за зрялост. С помощта на индекса се прави сравнение на нивата на способностите за киберсигурност за отделните държави и региони.

М10 – В индекса не се използват нива за оценяване на зрелостта на способностите за киберсигурност.

На базата на резултатите от направения сравнителен анализ могат да бъдат формулирани следните изводи:

- изследваните модели са разработени от научни организации в тясно сътрудничество и с помощта на академични организации, правителствени агенции и компании от частния бизнес. Това доказва както важността на въпроса за изграждане на адекватни способности за киберсигурност, така и всеобхватния характер на този въпрос;
- една част от анализираните модели са адресирани към измерване на способностите за киберсигурност на ниво компания, докато други модели позволяват измерване на зрелостта на способностите за киберсигурност на ниво държава;
- като обобщена цел за всички модели се поставя подпомагането на потребителите в процеса по изграждане и поддържане на способности за киберсигурност, приоритизиране на бъдещите усилия и проекти в сферата на киберсигурността, отстраняване на съществуващите слабости и пропуски;
- анализираните модели включват в структурата си различен брой области, с помощта на които се обхваща цялото поле на киберсигурността. Структурирането на тези области следва различна логика, която подпомага прилагането на всеки отделен модел в условията на конкретна среда;
- моделите, включени в изследването, използват нива на зрялост, с помощта на които се отчитат възможностите за извършване на различни дейности в полето на киберсигурността.

Направеният сравнителен анализ на модели за измерване на зрелостта на способностите за киберсигурност е полезен от една страна с конкретната информация за същността и особеностите на отделните модели, а от друга страна с посочване на неотложността и наложителността на измерването на способностите за киберсигурност на

държавните структури и на фирмите от частния сектор в България, както и на страната като цяло.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] George Sharkov, "Assessing the Maturity of National Cybersecurity and Resilience," Connections: The Quarterly Journal 19, no. 4 (2020): 5-24.

[2] ENISA, “CSIRT Maturity - Self-assessment Tool,” 2021, https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-capabilities/csirt-maturity/csirt-maturity-self-assessment-survey.

[3] ENISA, “NCSS: Practical Guide on Development and Execution,” 2012, https://www.enisa.europa.eu/ publications/national-cyber-security-strategies-an-implementation-guide.

[4] Gregory White, “The Community Cyber Security Maturity Model”, in 40th Hawaii International International Conference on Systems Science (HICSS-40 2007), 3-6 January 2007, Waikoloa, Big Island, HI, USA.

[5] National Institute of Standards and Technology, “Framework for Improving Critical Infrastructure Cybersecurity,” Version 1.1. 2018, Gaithersburg, http://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[6] International Telecommunication Union (ITU), “The Global Cybersecurity Index,” 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

[7] Institute of Internal Auditors, “Internal audit capability model (IA-CM) for the public sector: overview and application guide,” 2009, Altamonte Springs.

[8] “National Capabilities Assessment Framework,” European Union Agency for Cybersecurity (ENISA), 2020.